

JP 130 / US 0

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

J1000 U.S. PTO  
09/941898  
08/29/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日  
Date of Application:

2000年 8月31日

出 願 番 号  
Application Number:

特願2000-264521

出 願 人  
Applicant(s):

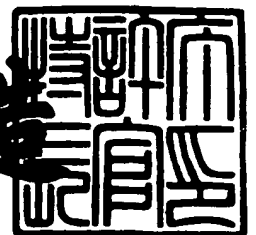
ソニー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 5月25日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 00005026

【提出日】 平成12年 8月31日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明の名称】 公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置、並びにプログラム提供媒体

【請求項の数】 22

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内

【氏名】 渡辺 秀明

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内

【氏名】 石橋 義人

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内

【氏名】 松山 科子

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内

【氏名】 二村 一郎

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内

【氏名】 昆 雅士

【特許出願人】

【識別番号】 000002185  
 【氏名又は名称】 ソニー株式会社  
 【代表者】 出井 伸之

【代理人】

【識別番号】 100101801  
 【弁理士】  
 【氏名又は名称】 山田 英治  
 【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100093241  
 【弁理士】  
 【氏名又は名称】 宮田 正昭  
 【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100086531  
 【弁理士】  
 【氏名又は名称】 澤田 俊夫  
 【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 062721  
 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1  
 【物件名】 図面 1  
 【物件名】 要約書 1  
 【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置、並びにプログラム提供媒体

【特許請求の範囲】

【請求項 1】

認証局の電子署名データを付加することにより暗号処理用の公開鍵の証明書として機能する公開鍵証明書を利用した公開鍵証明書利用システムであり、

公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報と、該公開鍵証明書の発行要求者の個人識別データとしてのテンプレートを格納した個人識別証明書から取得したテンプレートとの照合処理により個人認証を実行し、

該個人認証の成立を条件として、前記発行要求者の公開鍵証明書を発行する構成としたことを特徴とする公開鍵証明書利用システム。

【請求項 2】

前記個人認証は、公開鍵証明書の発行要求者の個人識別証明書を有する個人識別認証局において実行され、

前記個人識別認証局は、前記公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報を取得し、該サンプリング情報と前記個人識別証明書の格納テンプレートとの照合処理により個人認証を実行し、

前記個人認証の成立を前記認証局に通知することにより、該認証局において、前記発行要求者の公開鍵証明書を発行する構成としたことを特徴とする請求項 1 に記載の公開鍵証明書利用システム。

【請求項 3】

前記個人認証処理を実行する個人識別認証局は、

前記公開鍵証明書の発行要求者の個人識別証明書に基づく個人認証が成立したことを条件として、前記認証局との相互認証を実行し、該相互認証の成立を条件として、前記公開鍵証明書の発行要求者の公開鍵を認証局に送付し、該認証局は受領した公開鍵に対応する公開鍵証明書の生成を実行する構成であることを特徴とする請求項 1 に記載の公開鍵証明書利用システム。

【請求項 4】



前記認証局が、前記個人識別証明書に基づく個人認証に基づいて発行する公開鍵証明書は、1回の公開鍵使用処理でのみ有効なワンタイム公開鍵証明書として生成する構成であることを特徴とする請求項1に記載の公開鍵証明書利用システム。

【請求項5】

前記認証局、前記個人認証を実行する個人識別認証局のいずれも公開鍵証明書、あるいは個人識別証明書の利用当時者以外の第三者機関として構成されていることを特徴とする請求項1に記載の公開鍵証明書利用システム。

【請求項6】

前記公開鍵証明書利用システムにおいて、さらに、

前記個人認証処理を要求する認証要求デバイスを有し、

前記個人認証は、前記認証要求デバイスから前記個人認証を実行する個人識別認証局へのユーザ入力サンプリング情報の送付処理に基づいて実行され、該ユーザ入力サンプリング情報の送付処理は、前記認証要求デバイスと前記個人識別認証局との間の相互認証の成立を条件として実行する構成であることを特徴とする請求項1に記載の公開鍵証明書利用システム。

【請求項7】

前記公開鍵証明書利用システムにおいて、さらに、

サービスプロバイダに対するサービスリクエストを実行するユーザデバイスを有し、

該ユーザデバイスは、ユーザの入力サンプリング情報を、前記ユーザデバイスから前記個人認証を実行する個人識別認証局に対して送付され、

前記個人識別認証局はユーザ入力サンプリング情報を取得して、該サンプリング情報と前記個人識別証明書の格納テンプレートとの照合処理により個人認証を実行し、

前記個人識別認証局における個人認証成立を条件として、前記認証局において、前記ユーザの公開鍵証明書を前記ユーザデバイスに対して発行し、

前記公開鍵証明書を受領したユーザデバイスは、該公開鍵証明書を構成要素とするサービスリクエストを生成して前記サービスプロバイダに対して送付する処

理を実行する構成を有することを特徴とする請求項1に記載の公開鍵証明書利用システム。

【請求項8】

前記公開鍵証明書利用システムにおいて、さらに、

前記認証局の発行する公開鍵証明書は、公開鍵証明書の発行要求者の利用するユーザデバイスに対して発行され、該ユーザデバイスの記憶手段に格納され、

該ユーザデバイスは、該記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書の削除処理を実行する構成を有することを特徴とする請求項1に記載の公開鍵証明書利用システム。

【請求項9】

前記公開鍵証明書利用システムにおいて、さらに、

前記認証局の発行する公開鍵証明書は、公開鍵証明書の発行要求者の利用するユーザデバイスに対して発行され、該ユーザデバイスの記憶手段に格納され、

該ユーザデバイスは、該記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書、および公開鍵証明書に対応する公開鍵および秘密鍵の削除処理を実行する構成を有することを特徴とする請求項1に記載の公開鍵証明書利用システム。

【請求項10】

前記テンプレートは、個人の指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報等の生体情報、あるいは、印鑑、パスポート、免許書、カード等の非生体情報、あるいは、前記生体情報、非生体情報の2以上の組み合わせ情報、または前記各情報とパスワードとの組み合わせ情報のいずれかによって構成されたものであることを特徴とする請求項1に記載の公開鍵証明書利用システム。

【請求項11】

認証局の電子署名データを付加することにより暗号処理用の公開鍵の証明書として機能する公開鍵証明書を利用した公開鍵証明書利用方法であり、

公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報と、該公開鍵証明書の発行要求者の個人識別データとしてのテンプレートを格納した個人識別証明書から取得したテンプレートとの照合処理により個人認証を実行し、

該個人認証の成立を条件として、前記発行要求者の公開鍵証明書を発行することを特徴とする公開鍵証明書利用方法。

【請求項 1 2】

前記個人認証は、公開鍵証明書の発行要求者の個人識別証明書を有する個人識別認証局において実行され、

前記個人識別認証局は、前記公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報を取得し、該サンプリング情報と前記個人識別証明書の格納テンプレートとの照合処理により個人認証を実行し、

前記個人認証の成立を前記認証局に通知することにより、該認証局において、前記発行要求者の公開鍵証明書を発行することを特徴とする請求項 1 1 に記載の公開鍵証明書利用方法。

【請求項 1 3】

前記個人認証処理を実行する個人識別認証局は、

前記公開鍵証明書の発行要求者の個人識別証明書に基づく個人認証が成立したことを条件として、前記認証局との相互認証を実行し、該相互認証の成立を条件として、前記公開鍵証明書の発行要求者の公開鍵を認証局に送付し、該認証局は受領した公開鍵に対応する公開鍵証明書の生成を実行することを特徴とする請求項 1 1 に記載の公開鍵証明書利用方法。

【請求項 1 4】

前記認証局が、前記個人識別証明書に基づく個人認証に基づいて発行する公開鍵証明書は、1回の公開鍵使用処理でのみ有効なワンタイム公開鍵証明書として生成する構成であることを特徴とする請求項 1 1 に記載の公開鍵証明書利用方法。

【請求項 1 5】

前記認証局、前記個人認証を実行する個人識別認証局のいずれも公開鍵証明書、あるいは個人識別証明書の利用当時者以外の第三者機関として構成されていることを特徴とする請求項 1 1 に記載の公開鍵証明書利用方法。

【請求項 1 6】

前記公開鍵証明書利用方法において、さらに、

前記個人認証処理を要求する認証要求デバイスを有し、

前記個人認証は、前記認証要求デバイスから前記個人認証を実行する個人識別認証局へのユーザ入力サンプリング情報の送付処理に基づいて実行され、該ユーザ入力サンプリング情報の送付処理は、前記認証要求デバイスと前記個人識別認証局との間の相互認証の成立を条件として実行することを特徴とする請求項 1 1 に記載の公開鍵証明書利用方法。

【請求項 1 7】

前記公開鍵証明書利用方法において、さらに、

サービスプロバイダに対するサービスリクエストを実行するユーザデバイスを有し、

該ユーザデバイスは、ユーザの入力サンプリング情報を、前記ユーザデバイスから前記個人認証を実行する個人識別認証局に対して送付され、

前記個人識別認証局はユーザ入力サンプリング情報を取得して、該サンプリング情報と前記個人識別証明書の格納テンプレートとの照合処理により個人認証を実行し、

前記個人識別認証局における個人認証成立を条件として、前記認証局において、前記ユーザの公開鍵証明書を前記ユーザデバイスに対して発行し、

前記公開鍵証明書を受領したユーザデバイスは、該公開鍵証明書を構成要素とするサービスリクエストを生成して前記サービスプロバイダに対して送付する処理を実行することを特徴とする請求項 1 1 に記載の公開鍵証明書利用方法。

【請求項 1 8】

前記公開鍵証明書利用方法において、さらに、

前記認証局の発行する公開鍵証明書は、公開鍵証明書の発行要求者の利用するユーザデバイスに対して発行され、該ユーザデバイスの記憶手段に格納し、

該ユーザデバイスは、該記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書の削除処理を実行することを特徴とする請求項 1 1 に記載の公開鍵証明書利用方法。

【請求項 1 9】

前記公開鍵証明書利用方法において、さらに、

前記認証局の発行する公開鍵証明書は、公開鍵証明書の発行要求者の利用するユーザデバイスに対して発行され、該ユーザデバイスの記憶手段に格納し、

該ユーザデバイスは、該記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書、および公開鍵証明書に対応する公開鍵および秘密鍵の削除処理を実行することを特徴とする請求項 11 に記載の公開鍵証明書利用方法。

【請求項 20】

情報処理装置において、

個人識別認証局によるユーザサンプリング情報と個人識別証明書の格納テンプレートとの照合処理による個人認証成立を条件として、ユーザに対して発行される公開鍵証明書を受領し、該情報処理装置の記憶手段に格納する処理を実行するとともに、

前記記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書の削除処理を実行する構成を有することを特徴とする情報処理装置。

【請求項 21】

前記情報処理装置は、

前記記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書、および公開鍵証明書に対応する公開鍵および秘密鍵の削除処理を実行する構成を有することを特徴とする請求項 20 に記載の情報処理装置。

【請求項 22】

認証局の電子署名データを付加することにより暗号処理用の公開鍵の証明書として機能する公開鍵証明書を利用したデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報と、該公開鍵証明書の発行要求者の個人識別データとしてのテンプレートを格納した個人識別証明書から取得したテンプレートとの照合処理による個人認証実行ステップと、

前記個人認証の成立を条件とする前記発行要求者の公開鍵証明書発行ステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置、並びにプログラム提供媒体に関する。特に、インターネット等の通信ネットワークあるいは媒体を介するデータ通信において、通信相手の個人識別としての個人認証処理を実行し、その後の公開鍵の利用を効率的に実行することを可能とした公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置、並びにプログラム提供媒体に関する。

【0002】

【従来の技術】

企業あるいは個人においてデータ処理装置、例えばパーソナルコンピュータ（PC）等の様々なデータ処理装置が盛んに使用され、このような装置には様々な機密データが格納される場合がある。このような機密情報に対する不正なユーザのアクセスを排除するため、PCに格納された情報の漏洩を防止する技術が開発されており、例えば、パスワード入力、ユーザの生体情報によるユーザ識別処理等が開発されている。

【0003】

さらに、昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体（メディア）を介して流通している。このような状況の中で、コンテンツの配布あるいはコンテンツ利用料金の回収等、様々な処理において、ユーザ識別処理を確実に迅速に実行し、かつ、識別処理において用いられる個人情報の漏洩の防止が重要な課題となっている。

【0004】

一般的なユーザ識別方法としては、例えばユーザID、パスワード等を予め設定し、設定データと入力データとを照合する処理方法がある。しかし、この方法

は、登録されているユーザID、パスワードの漏洩のおそれが常に存在し、一旦漏洩した場合には、同一のユーザID、パスワードの使用は不可能となる。このような問題点を解決する手法として、生体情報を用いたユーザ識別手法がある。

#### 【0005】

従来から行われている生体情報を用いた個人識別処理の一例について説明する。代表的例として指紋読み取り照合処理を実行する個人認証装置について図1を用いて説明する。図1に示すPC20の利用者は、予め、個人の指紋情報を読み取り装置を持つ個人認証装置10に登録し、このデータをセキュアメモリ14内に格納する。格納された指紋情報をテンプレート (Template) と呼ぶ。ユーザはパソコン20などのデータを利用する際に、指紋読み取り装置として構成された個人認証装置10により指紋の照合処理を実行させる。

#### 【0006】

ユーザは、例えばCCDカメラによって構成される個人情報取得部11において指紋情報の読み取りを実行する。読み取られた指紋情報は、情報変換部12で特徴抽出処理が実行され、比較部13にて、セキュアメモリ14に格納されたテンプレートと、個人情報取得部11で取得され、特徴抽出されたデータとの比較処理が行われる。

#### 【0007】

比較部13における比較処理においては、比較部に予め設定したしきい値により一致、不一致の判定がコントロールされる。比較対照の両データが設定しきい値を越えて一致していればOK、しきい値以下の一致度であればNGとなる。なお、指紋情報は指紋画像データそのもので、情報変換部12で特徴抽出されたデータと、この画像データの比較を行い、しきい値と比較することになる。

#### 【0008】

比較部13での判定処理において、入力情報と登録情報が一致すると判定された場合には、通信部16を経由してパソコン20に照合成功が伝えられ、PC20に対するアクセスが許可される。一致していないと判定された場合には照合失敗が伝えられ、PC20に対するアクセスが拒否される。なお、個人認証装置10は、図1に示すように複数のユーザ (ユーザID=ID1~IDn) の指紋情

報テンプレートをセキュアメモリに格納し、いずれかの格納テンプレートと一致したことを条件としてPCのアクセスを許可する構成とすることで、一台の個人認証装置で複数のユーザに対応することが可能となる。

【0009】

【発明が解決しようとする課題】

しかしながら、このような個人認証装置では、テンプレートは指紋読み取り照合装置内のメモリに保存される構成であり、以下のような問題点がある。

(a) 照合結果を利用するには、テンプレートを保持している指紋読み取り照合装置を使用する必要がある。

(b) 複数の場所で指紋照合を行う場合、あらかじめ複数の指紋読み取り照合装置に指紋登録を行なう必要がある。

(c) テンプレートが指紋読み取り照合装置内にあるため、テンプレート情報としてのデータを改竄、読み取りされる危険がある。

(d) 照合結果をPC等に転送しているため、その結果を攻撃されやすい。

【0010】

このように、従来の個人認証システムは、機密情報を扱う特定のPC等のデータ処理装置に不可分に構成され、そのPCを扱うユーザ専用の認証に重点が置かれており、テンプレートを保存していない機器を使用する場合の認証には全く利用できない。また、テンプレートを格納しているのは指紋読み取り照合装置自体であり、テンプレートの安全性、信頼性といった面で問題がある。

【0011】

さらに、昨今の暗号化データを使用したネットワークを介するデータ送受信、あるいは媒体を介するデータ配信においては、公開鍵暗号方式による暗号処理、および公開鍵の信頼性を保証する公開鍵証明書が多く使用されている。しかしながら、公開鍵証明書は、公開鍵の保証を行なうものの、公開鍵とその公開鍵の所有者である個人の結び付きを保証することはできないという問題点がある。すなわち、

(e) 暗号化データの送信等に使用される公開鍵証明書とその公開鍵の所有者個人との関係を保証する方法がなく、公開鍵の所有者の識別手段が十分ではなかつ



た。

【 0 0 1 2 】

このように、従来の個人認証システムには、様々な解決すべき問題点が存在する。特に、昨今のインターネット等、通信システムの発達したネットワーク社会においては、様々な場所、時間に、多様な通信機器、データ処理機器を用いて機密情報、個人情報を扱う機会が増大している。また、特定のユーザ、例えば会員向けのコンテンツ配信、有料コンテンツの配信システム、サービス等においては、コンテンツ、サービスの配信時にユーザの識別処理を実行することが必要となる。このような状況において、場所、時間、使用機器等の環境に依存しない個人認証処理システムの実現要求が高まっている。

【 0 0 1 3 】

本発明は、上述の状況に鑑みてなされたものであり、個人認証を様々な環境下において実行でき、さらに個人認証の信頼性を高め、安全なテンプレート情報の格納、利用形態を実現し、さらに公開鍵証明書との関連した使用態様を実現することにより、個人認証の多様な分野での利用を可能とした公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置を提供することを目的とする。

【 0 0 1 4 】

特に、本発明は、インターネット等の通信ネットワークあるいは媒体を介するデータ通信において、通信相手の個人識別としての個人認証処理を実行し、その後の公開鍵の利用を効率的に実行することを可能とした公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置を提供することを目的とする。

【 0 0 1 5 】

【課題を解決するための手段】

本発明の第1の側面は、

認証局の電子署名データを付加することにより暗号処理用の公開鍵の証明書として機能する公開鍵証明書を利用した公開鍵証明書利用システムであり、

公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報と、該公開鍵証明書の発行要求者の個人識別データとしてのテンプレートを格納した個

人識別証明書から取得したテンプレートとの照合処理により個人認証を実行し、

該個人認証の成立を条件として、前記発行要求者の公開鍵証明書を発行する構成としたことを特徴とする公開鍵証明書利用システムにある。

【 0 0 1 6 】

さらに、本発明の公開鍵証明書利用システムの一実施態様において、前記個人認証は、公開鍵証明書の発行要求者の個人識別証明書を有する個人識別認証局において実行され、前記個人識別認証局は、前記公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報を取得し、該サンプリング情報と前記個人識別証明書の格納テンプレートとの照合処理により個人認証を実行し、前記個人認証の成立を前記認証局に通知することにより、該認証局において、前記発行要求者の公開鍵証明書を発行する構成としたことを特徴とする。

【 0 0 1 7 】

さらに、本発明の公開鍵証明書利用システムの一実施態様において、前記個人認証処理を実行する個人識別認証局は、前記公開鍵証明書の発行要求者の個人識別証明書に基づく個人認証が成立したことを条件として、前記認証局との相互認証を実行し、該相互認証の成立を条件として、前記公開鍵証明書の発行要求者の公開鍵を認証局に送付し、該認証局は受領した公開鍵に対応する公開鍵証明書の生成を実行する構成であることを特徴とする。

【 0 0 1 8 】

さらに、本発明の公開鍵証明書利用システムの一実施態様において、前記認証局が、前記個人識別証明書に基づく個人認証に基づいて発行する公開鍵証明書は、1回の公開鍵使用処理でのみ有効なワンタイム公開鍵証明書として生成する構成であることを特徴とする。

【 0 0 1 9 】

さらに、本発明の公開鍵証明書利用システムの一実施態様において、前記認証局、前記個人認証を実行する個人識別認証局のいずれも公開鍵証明書、あるいは個人識別証明書の利用当時者以外の第三者機関として構成されていることを特徴とする。

【 0 0 2 0 】

さらに、本発明の公開鍵証明書利用システムの一実施態様において、前記公開鍵証明書利用システムにおいて、さらに、前記個人認証処理を要求する認証要求デバイスを有し、前記個人認証は、前記認証要求デバイスから前記個人認証を実行する個人識別認証局へのユーザ入力サンプリング情報の送付処理に基づいて実行され、該ユーザ入力サンプリング情報の送付処理は、前記認証要求デバイスと前記個人識別認証局との間の相互認証の成立を条件として実行する構成であることを特徴とする。

## 【 0 0 2 1 】

さらに、本発明の公開鍵証明書利用システムの一実施態様において、前記公開鍵証明書利用システムにおいて、さらに、サービスプロバイダに対するサービスリクエストを実行するユーザデバイスを有し、該ユーザデバイスは、ユーザの入力サンプリング情報を、前記ユーザデバイスから前記個人認証を実行する個人識別認証局に対して送付され、前記個人識別認証局はユーザ入力サンプリング情報を取得して、該サンプリング情報と前記個人識別証明書の格納テンプレートとの照合処理により個人認証を実行し、前記個人識別認証局における個人認証成立を条件として、前記認証局において、前記ユーザの公開鍵証明書を前記ユーザデバイスに対して発行し、前記公開鍵証明書を受領したユーザデバイスは、該公開鍵証明書を構成要素とするサービスリクエストを生成して前記サービスプロバイダに対して送付する処理を実行する構成を有することを特徴とする。

## 【 0 0 2 2 】

さらに、本発明の公開鍵証明書利用システムの一実施態様において、前記公開鍵証明書利用システムにおいて、さらに、前記認証局の発行する公開鍵証明書は、公開鍵証明書の発行要求者の利用するユーザデバイスに対して発行され、該ユーザデバイスの記憶手段に格納され、該ユーザデバイスは、該記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書の削除処理を実行する構成を有することを特徴とする。

## 【 0 0 2 3 】

さらに、本発明の公開鍵証明書利用システムの一実施態様において、前記公開鍵証明書利用システムにおいて、さらに、前記認証局の発行する公開鍵証明書は

、公開鍵証明書の発行要求者の利用するユーザデバイスに対して発行され、該ユーザデバイスの記憶手段に格納され、該ユーザデバイスは、該記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書、および公開鍵証明書に対応する公開鍵および秘密鍵の削除処理を実行する構成を有することを特徴とする。

【 0 0 2 4 】

さらに、本発明の公開鍵証明書利用システムの一実施態様において、前記テンプレートは、個人の指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報等の生体情報、あるいは、印鑑、パスポート、免許書、カード等の非生体情報、あるいは、前記生体情報、非生体情報の2以上の組み合わせ情報、または前記各情報とパスワードとの組み合わせ情報のいずれかによって構成されたものであることを特徴とする。

【 0 0 2 5 】

さらに、本発明の第2の側面は、

認証局の電子署名データを付加することにより暗号処理用の公開鍵の証明書として機能する公開鍵証明書を利用した公開鍵証明書利用方法であり、

公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報と、該公開鍵証明書の発行要求者の個人識別データとしてのテンプレートを格納した個人識別証明書から取得したテンプレートとの照合処理により個人認証を実行し、

該個人認証の成立を条件として、前記発行要求者の公開鍵証明書を発行することを特徴とする公開鍵証明書利用方法にある。

【 0 0 2 6 】

さらに、本発明の公開鍵証明書利用方法の一実施態様において、前記個人認証は、公開鍵証明書の発行要求者の個人識別証明書を有する個人識別認証局において実行され、前記個人識別認証局は、前記公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報を取得し、該サンプリング情報と前記個人識別証明書の格納テンプレートとの照合処理により個人認証を実行し、前記個人認証の成立を前記認証局に通知することにより、該認証局において、前記発行要求者の公開鍵証明書を発行することを特徴とする。

## 【 0 0 2 7 】

さらに、本発明の公開鍵証明書利用方法の一実施態様において、前記個人認証処理を実行する個人識別認証局は、前記公開鍵証明書の発行要求者の個人識別証明書に基づく個人認証が成立したことを条件として、前記認証局との相互認証を実行し、該相互認証の成立を条件として、前記公開鍵証明書の発行要求者の公開鍵を認証局に送付し、該認証局は受領した公開鍵に対応する公開鍵証明書の生成を実行することを特徴とする。

## 【 0 0 2 8 】

さらに、本発明の公開鍵証明書利用方法の一実施態様において、前記認証局が、前記個人識別証明書に基づく個人認証に基づいて発行する公開鍵証明書は、1回の公開鍵使用処理でのみ有効なワンタイム公開鍵証明書として生成する構成であることを特徴とする。

## 【 0 0 2 9 】

さらに、本発明の公開鍵証明書利用方法の一実施態様において、前記認証局、前記個人認証を実行する個人識別認証局のいずれも公開鍵証明書、あるいは個人識別証明書の利用当時者以外の第三者機関として構成されていることを特徴とする。

## 【 0 0 3 0 】

さらに、本発明の公開鍵証明書利用方法の一実施態様において、前記公開鍵証明書利用方法において、さらに、前記個人認証処理を要求する認証要求デバイスを有し、前記個人認証は、前記認証要求デバイスから前記個人認証を実行する個人識別認証局へのユーザ入力サンプリング情報の送付処理に基づいて実行され、該ユーザ入力サンプリング情報の送付処理は、前記認証要求デバイスと前記個人識別認証局との間の相互認証の成立を条件として実行することを特徴とする。

## 【 0 0 3 1 】

さらに、本発明の公開鍵証明書利用方法の一実施態様において、前記公開鍵証明書利用方法において、さらに、サービスプロバイダに対するサービスリクエストを実行するユーザデバイスを有し、該ユーザデバイスは、ユーザの入力サンプリング情報を、前記ユーザデバイスから前記個人認証を実行する個人識別認証局

に対して送付され、前記個人識別認証局はユーザ入力サンプリング情報を取得して、該サンプリング情報と前記個人識別証明書の格納テンプレートとの照合処理により個人認証を実行し、前記個人識別認証局における個人認証成立を条件として、前記認証局において、前記ユーザの公開鍵証明書を前記ユーザデバイスに対して発行し、前記公開鍵証明書を受領したユーザデバイスは、該公開鍵証明書を構成要素とするサービスリクエストを生成して前記サービスプロバイダに対して送付する処理を実行することを特徴とする。

【 0 0 3 2 】

さらに、本発明の公開鍵証明書利用方法の一実施態様において、前記公開鍵証明書利用方法において、さらに、前記認証局の発行する公開鍵証明書は、公開鍵証明書の発行要求者の利用するユーザデバイスに対して発行され、該ユーザデバイスの記憶手段に格納し、該ユーザデバイスは、該記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書の削除処理を実行することを特徴とする。

【 0 0 3 3 】

さらに、本発明の公開鍵証明書利用方法の一実施態様において、前記公開鍵証明書利用方法において、さらに、前記認証局の発行する公開鍵証明書は、公開鍵証明書の発行要求者の利用するユーザデバイスに対して発行され、該ユーザデバイスの記憶手段に格納し、

該ユーザデバイスは、該記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書、および公開鍵証明書に対応する公開鍵および秘密鍵の削除処理を実行することを特徴とする。

【 0 0 3 4 】

さらに、本発明の第3の側面は、  
情報処理装置において、

個人識別認証局によるユーザサンプリング情報と個人識別証明書の格納テンプレートとの照合処理による個人認証成立を条件として、ユーザに対して発行される公開鍵証明書を受領し、該情報処理装置の記憶手段に格納する処理を実行するとともに、

前記記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書の削除処理を実行する構成を有することを特徴とする情報処理装置にある。

【 0 0 3 5 】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記記憶手段に格納された公開鍵証明書の利用処理完了に伴い、該公開鍵証明書、および公開鍵証明書に対応する公開鍵および秘密鍵の削除処理を実行する構成を有することを特徴とする。

【 0 0 3 6 】

さらに、本発明第4の側面は、

認証局の電子署名データを付加することにより暗号処理用の公開鍵の証明書として機能する公開鍵証明書を利用したデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

公開鍵証明書の発行要求者の個人識別データとしてのサンプリング情報と、該公開鍵証明書の発行要求者の個人識別データとしてのテンプレートを格納した個人識別証明書から取得したテンプレートとの照合処理による個人認証実行ステップと、

前記個人認証の成立を条件とする前記発行要求者の公開鍵証明書発行ステップと、

を有することを特徴とするプログラム提供媒体にある。

【 0 0 3 7 】

本発明の第4の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MO、DVDなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【 0 0 3 8 】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供

媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【 0 0 3 9 】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。

【 0 0 4 0 】

【実施例】

以下、本発明の構成について、下記の項目順に説明する。

1. 本発明の概念と証明書概要
2. テンプレートの暗号化
3. テンプレート、個人識別証明書（IDC）の登録、変更処理
4. 個人識別証明書（IDC）の基本的利用形態
5. 個人識別証明書（IDC）を使用した認証処理態様
6. 個人識別証明書に基づくユーザ認証によるコンテンツの利用権制御処理
7. 個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンク
8. 個人識別証明書（IDC）による認証と公開鍵証明書（PKC）に基づく

コンテンツ利用処理

9. ワンタイム公開鍵証明書（ワンタイムPKC）
10. 照合証明書
11. 個人識別証明書（IDC）のダウンロードおよびコンテンツ利用処理
12. 個人識別証明書（IDC）の有効期限設定

【 0 0 4 1 】

[ 1. 本発明の概念と証明書概要 ]

( 1. 1. 本発明のシステムの基本概念 )

まず、本発明の個人認証システムの基本概念について説明する。本発明の個人



認証は個人識別証明書（IDC：Identification Certificate）を使用することによって実現される。個人識別証明書（IDC）は、信頼できる第三者機関である個人識別認証局（IDA：Identification Authority）が証明対象となる個人各々について、個人の確認を行なった上で発行する証明書である。

【0042】

個人識別証明書（IDC）には、各個人を識別するための情報（テンプレート情報）が格納される。個人識別情報としては、例えば指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報が使用可能であり、さらに生体情報以外の個人識別情報、例えば印鑑、パスポート、免許書、カード等の識別データ、あるいは、上記各情報の組合わせ、または、上記各情報とパスワードとの組み合わせ等、基本的に本人のみが持ち得る情報が使用され、これらの個人識別情報が原則として暗号化されて、テンプレート情報として格納される。

【0043】

個人識別認証局（IDA）により発行された個人識別証明書（IDC）は、その登録者自身であるユーザ、または登録者であるユーザに対してコンテンツ配信を行なうサービスプロバイダ（SP）、あるいは利用者確認を必要とする様々な機関（例えば決済金融機関等）、あるいはユーザデバイスからの要求に応じて、個人識別認証局（IDA）から提供され、個人識別のために利用される。具体的な利用形態については、後段で詳細に説明する。

【0044】

さらに、本発明の個人識別証明書（IDC）は、公開鍵証明書（PKC：Public Key Certificate）との組み合わせにおいて有効な利用形態が実現される。すなわち、コンテンツの暗号化配信を行なうサービスプロバイダ（SP）が個人の識別処理を行う際に個人識別証明書（IDC）を利用し、識別された個人にのみ復号可能な暗号化データの配信を公開鍵証明書を用いた公開鍵暗号方式により行なうことを可能とする。

【0045】

図2に本発明の個人認証システムを利用し、かつ公開鍵証明書を用いた暗号化データ通信の概略を説明する図を示す。上述の個人識別証明書（IDC）を発行

する個人識別認証局（IDA）201、また公開鍵証明書（PKC）を発行する認証局（CA：Certificate Authority）202においてそれぞれの証明書が所定の手続きにより発行される。

【0046】

暗号化データ通信は、例えばコンテンツ配信を行なうサービスプロバイダ（SP）203と、ユーザデバイスA205の間において実行される。この際、サービスプロバイダ（SP）203は、ユーザデバイスAの使用者がユーザAであることを確認し、ユーザAにおいて復号可能な暗号化データを生成してコンテンツの暗号化配信を行なう。

【0047】

ユーザAは、個人情報を個人識別認証局（IDA）201に登録することにより、個人識別認証局（IDA）201から個人識別証明書（IDC）の発行を受けており、個人識別証明書（IDC）により、サービスプロバイダ（SP）203はユーザAであることの確認を行なう。この場合、サービスプロバイダ（SP）203が個人識別証明書（IDC）による個人認証を実行するエンティティとなる。個人識別証明書による確認処理態様には各種あるが、これらについては後段で詳細に説明する。

【0048】

また、ユーザAは、ユーザ自身の公開鍵を認証局202に提出し、認証局の電子署名入りの公開鍵証明書の発行を受ける。サービスプロバイダ（SP）203が個人識別証明書（IDC）に基づいてユーザAであることの確認を行なった後、例えば、サービスプロバイダ（SP）203は、ユーザAの公開鍵証明書から公開鍵を取り出して、取り出した公開鍵によってコンテンツを暗号化して、コンテンツをユーザAに対して配信する。暗号化コンテンツの配信を受けたユーザデバイスA205のユーザAは、公開鍵とペアになった秘密鍵によって配信された暗号化データを復号して利用する。

【0049】

また、決済機関としてのサービスプロバイダ（SP）204と、ユーザデバイスB206との間においても、上述と同様にサービスプロバイダ（SP）204

によるユーザ B の個人識別証明書に基づくユーザ B の確認、さらにユーザ B の公開鍵証明書を用いた暗号化データ（例えばコンテンツデータ、決済データ等）の送受信が行われる。この場合、ユーザデバイスが個人識別証明書（IDC）による個人認証を実行するエンティティとなる。

#### 【0050】

さらに、ユーザデバイス A 205 と、ユーザデバイス B 206 との間のデータ通信においても、ユーザ A、B の個人識別証明書に基づくユーザ A、B の確認、ユーザ A またはユーザ B の公開鍵証明書を用いた暗号化データの送受信が行われる。

#### 【0051】

このように、様々な形態でのデータ送受信において、個人識別証明書および公開鍵証明書が利用可能である。個人識別証明書単独の利用形態も可能であり、機密情報を格納した PC 等に対するアクセス時に個人識別証明書による照合処理によりユーザ確認を行なうことももちろん可能である。個人識別証明書による個人認証を実行するエンティティは、サービスプロバイダ（SP）、ユーザデバイス、さらに個人識別認証局（IDA）等、様々なエンティティである。

#### 【0052】

また、図 2 に示すように、本発明のシステムの一実施例として、個人識別認証局（IDA）201 の発行する個人識別証明書（IDC）と、認証局 202 の発行する公開鍵証明書（PKC）をリンクさせた構成がある。リンク構成には、個人識別証明書の中に公開鍵証明書（PKC）を含ませる構成としたり、リンク情報体としての組情報を生成する構成等がある。これらのリンク構成については、後段で詳細に説明する。

#### 【0053】

上述の説明における公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。公開鍵暗号方式では、暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号化方式と異なり、秘密に保つ必要のある秘密鍵は、特定の 1 人が持てばよいための鍵の管理において有利である。公開鍵暗号方式の代表的な

ものには R S A (Rivest-Shamir-Adleman) 暗号がある。これは非常に大きな 2 つの素数 (例えば 1 5 0 桁) の積を用いるものであり、大きな 2 つの素数 (例えば 1 5 0 桁) の積の素因数分解処理の困難性を利用している。

#### 【 0 0 5 4 】

公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者 A が公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者 A は公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者 A に送付する。利用者 A は秘密鍵を用いて暗号化文書等を復号する等のシステムである。また、利用者 A は、秘密鍵を用いて文書等に署名を付け、不特定のユーザが公開鍵証明書から所定の手続きを経て公開鍵を入手して、その署名の検証を行なうことができる。以下、本発明の個人認証システムの具体的説明に先立ち、本発明のシステムにおいて用いられる公開鍵証明書 (P K C) および個人識別証明書 (I D C) のデータ構成について説明する。

#### 【 0 0 5 5 】

##### (1. 2. 公開鍵証明書)

公開鍵証明書について図 3, 4 を用いて説明する。公開鍵証明書は、公開鍵暗号方式における認証局 (C A : Certificate Authority または I A : Issuer Authority) が発行する証明書であり、ユーザが自己の I D、公開鍵等を認証局に提出することにより、認証局側が認証局の I D や有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

#### 【 0 0 5 6 】

公開鍵証明書のフォーマット例を示す。これは、公開鍵証明書フォーマット X . 5 0 9 V 3 に準拠した例である。

#### 【 0 0 5 7 】

バージョン (version) は、証明書フォーマットのバージョンを示す。

シリアルナンバ (Serial Number) は、公開鍵証明書発行局 (I A) によって

設定される公開鍵証明書のシリアルナンバである。

署名アルゴリズム識別子、アルゴリズムパラメータ (Signature algorithm Identifier algorithm parameter) は、公開鍵証明書の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号および R S A があり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、R S A が適用されている場合には鍵長が記録される。

発行者 (issuer) は、公開鍵証明書の発行者、すなわち公開鍵証明書発行局 (I A) の名称が識別可能な形式 (Distinguished Name) で記録されるフィールドである。

有効期限 (validity) は、証明書の有効期限である開始日時、終了日時が記録される。

サブジェクト (subject) は、ユーザである認証対象者の名前が記録される。具体的には例えばユーザ機器の I D や、サービス提供主体の I D 等である。

サブジェクト公開鍵情報 (subject Public Key Info algorithm subject Public key) は、ユーザの公開鍵情報としての鍵アルゴリズム、鍵情報そのものを格納するフィールドである。

#### 【 0 0 5 8 】

ここまでの、公開鍵証明書フォーマット X. 5 0 9 V 1 に含まれるフィールドであり、以下は、公開鍵証明書フォーマット X. 5 0 9 V 3 において追加されるフィールドである。

#### 【 0 0 5 9 】

証明局鍵識別子 (authority Key Identifier—key Identifier, authority Certificate Issuer, authority Certificate Serial Number) は、公開鍵証明書発行局 (I A) の鍵を識別する情報であり、鍵識別番号 (8 進数)、公開鍵証明書発行局 (I A) の名称、認証番号を格納する。

サブジェクト鍵識別子 (subject key Identifier) は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を格納する。

鍵使用目的 (key usage) は、鍵の使用目的を指定するフィールドであり、( 0 ) デジタル署名用、( 1 ) 否認防止用、( 2 ) 鍵の暗号化用、( 3 ) メッセ

ージの暗号化用、(4) 共通鍵配送用、(5) 認証の署名確認用、(6) 失効リストの署名確認用の各使用目的が設定される。

秘密鍵有効期限(private Key Usage Period)は、ユーザの有する秘密鍵の有効期限を記録する。

認証局ポリシー (certificate Policies) は、認証局、ここでは、公開鍵証明書発行局 (I A) および登録局 (R A) の証明書発行ポリシーを記録する。例えば I S O / I E C 9 3 8 4 - 1 に準拠したポリシー I D、認証基準である。

ポリシー・マッピング (policy Mapping) は、C A (公開鍵証明書発行局 (I A)) を認証する場合にのみ記録するフィールドであり、証明書発行を行なう公開鍵証明書発行局 (I A) のポリシーと、被認証ポリシーのマッピングを規定する。

サポート・アルゴリズム (supported Algorithms) は、ディレクトリ (X. 5 0 0) のアトリビュートを定義する。これは、コミュニケーションの相手がディレクトリ情報を利用する場合に、事前にそのアトリビュートを知らせるのに用いる。

サブジェクト別名 (subject Alt Name) は、ユーザの別名を記録するフィールドである。

発行者別名 (issuer Alt Name) は、証明書発行者の別名を記録するフィールドである。

サブジェクト・ディレクトリ・アトリビュート (subject Directory Attribute) は、ユーザの任意の属性を記録するフィールドである。

基本制約 (basic Constraint) は、証明対象の公開鍵が認証局 (公開鍵証明書発行局 (I A)) の署名用か、ユーザのものをかを区別するためのフィールドである。

許容サブツリー制約名 (name Constraints permitted Subtrees) は、被認証者が認証局 (公開鍵証明書発行局 (I A)) である場合にのみ使用される証明書の有効領域を示すフィールドである。

制約ポリシー (policy Constraints) は、認証パスの残りに対する明確な認証ポリシー I D、禁止ポリシーマップを要求する制限を記述する。

C R L 参照ポイント (Certificate Revocation List Distribution Points) は、ユーザが証明書を利用する際に、証明書が失効していないか、どうかを確認するための失効リスト (図 9 参照) の参照ポイントを記述するフィールドである。

署名は、公開鍵証明書発行者 (公開鍵証明書発行局 (I A)) の署名フィールドである。電子署名は、証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

#### 【 0 0 6 0 】

認証局は、図 3, 4 に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布 (これをリボケーション: Revocation と呼ぶ) を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

#### 【 0 0 6 1 】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

#### 【 0 0 6 2 】

##### ( 1 . 3 . 個人識別証明書 )

本発明の個人認証システムにおいて用いられる個人識別証明書 (I D C) には、個人識別のための情報 (以下、この I D C に含まれる個人識別情報をテンプレート情報と呼ぶ) が含まれる。テンプレート情報は、個人の生体 (バイオメトリクス) 情報、例えば指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報が使用可能であり、さらに生体情報以外の個人識別情報、例えば印鑑、パスポート、免許書、カード等の識別データ、あるいは、上記各情報の組み合わせ、または、上記各情報とパスワードとの組み合わせ等、基本的に本人のみが持ち得る情報が使用可能である。このようなテンプレート情報は、不正な第三者に漏洩することがな

いように暗号化してIDCに格納することが望ましい。ただし、個人識別証明書の流通範囲が極めて限定され、秘密の漏洩防止が確実に実現されることが保証される環境であれば、テンプレートの暗号化は必ずしも必要ではない。

#### 【0063】

また、個人識別証明書（IDC）には、個人識別認証局（IDA）のデジタル署名がなされ、個人識別証明書の改竄が防止される構成となっている。

#### 【0064】

個人識別証明書のフォーマット例を図5に示す。図5の個人識別証明書は、必須項目フィールドと、拡張項目フィールド、そして、署名フィールドに大別される。各項目について説明する。

#### 【0065】

まず、必須項目の各フィールドについて説明する。

バージョン（version）は、証明書フォーマットのバージョンを示す。

認証番号（Serial Number）は、個人識別認証局（IDA）によって設定される各個人識別証明書（IDC）のシリアルナンバである。

署名方式（Signature algorithm Identifier algorithm parameter）は、個人識別証明書の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびRSAがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、RSAが適用されている場合には鍵長が記録される。

発行者（issuer）は、個人識別証明書の発行者、すなわち個人識別認証局（IDA）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。

有効期限（validity）は、証明書の有効期限である開始日時、終了日時が記録される。

サブジェクト（subject）は、ユーザである認証対象者の名前が記録される。具体的には例えばユーザのIDや、氏名等である。

テンプレート情報（Subject Template Info）は、ユーザの個人識別情報として、例えば前述した指紋等の生体情報のデータを暗号化して格納するフィールド



であり、テンプレートの暗号化方式、暗号化するために使用した公開鍵証明書の固有識別子（ID）または認証番号、暗号化アルゴリズム、パラメータ、テンプレートの有効期限としての開始日時、終了日時、テンプレートの種別、テンプレート（暗号化）の各情報が格納される。

ここまでが、必須項目フィールドとして設定される。

#### 【0066】

以下は、個人識別証明書（IDC）における拡張フィールドである。

被認証者の公開鍵証明書情報（Subject PKC info）には、被認証者の公開鍵証明書情報としての、被認証者の公開鍵証明書の認証番号、被認証者の公開鍵証明書の被認証者固有IDが格納される。

個人識別認証局の固有ID（Issuer Unique ID）は、個人識別認証局（IDA）の固有IDを格納する。

被認証者の固有ID（Subject Unique ID）は、被認証者の固有IDを格納する。

公開鍵証明書（Public Key Certificate）は、前述した公開鍵証明書を格納する。

個人識別認証局の別名（Issuer Alt Name）は、個人識別認証局の別名を格納する。

個人情報（Subject Directory Attribute）は、本人確認のための情報として、ユーザの任意の属性、例えば、年齢、性別、住所、電話番号等の個人情報が必要に応じて暗号化されて格納される。

有効回数（Valid Count）は、個人識別証明書による個人認証処理の制限回数を記録するフィールドである。1度発行した証明書の利用を制限回数内にとどめるための設定数を記録する。

組情報へのリンク情報（Control Table link Info）は、個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンク情報としての組情報を格納する。例えば、個人識別証明書による個人認証処理を条件として実行されるデータ通信、データ処理において使用される公開鍵証明書とのリンク情報を格納する。リンク情報、組情報については後段で詳細に説明する。

以上が、個人識別証明書（IDC）における拡張フィールドの内容である。

【0067】

電子署名は、証明書を構成する各フィールドの全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して個人識別認証局（IDA）の秘密鍵を用いて生成したデータである。

【0068】

なお、個人識別証明書（IDC）における拡張フィールドには、さらに他の情報を格納してもよい。例えばテンプレート情報を公開鍵ではなく共通の秘密鍵で暗号化し、その暗号化に用いた共通鍵をユーザデバイス、サービスプロバイダ、または個人識別認証局（IDA）の公開鍵で暗号化して格納してもよい。この場合の処理形態については後述する。

【0069】

[2. テンプレートの暗号化]

上述の個人識別証明書（IDC）には、個人識別のための情報（テンプレート情報）が含まれる。テンプレート情報は、前述したように、個人の生体（バイオメトリクス）情報、例えば指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報を使用可能であり、さらに生体情報以外の個人識別情報、例えば印鑑、パスポート、免許書、カード等の識別データ、あるいは、上記各情報の組み合わせ、または、上記各情報とパスワードとの組み合わせ等、基本的に本人のみが持ち得る情報であり個人の識別の基礎となる情報である。

【0070】

テンプレートは、前述したように特定の機密の守られる範囲内での証明書使用に限定される場合以外においては、第三者に対する漏洩を防止するため、暗号化して格納することが望ましい。ここでは、テンプレートの格納態様、暗号化態様について説明する。

【0071】

テンプレートの格納および暗号化態様としては、以下の態様がある。

- 1) テンプレートを暗号化しないで格納する。
- 2) テンプレートをユーザ（個人識別証明書において識別されるユーザ）の公

公開鍵で暗号化する。

3) テンプレートを共通鍵  $K_t$  で暗号化し共通鍵  $K_t$  をユーザの公開鍵で暗号化する。

4) テンプレートをサービスプロバイダ (SP) (個人識別証明書を利用してサービス提供ユーザの識別を実行する SP) の公開鍵で暗号化する。

5) テンプレートを共通鍵  $K_t$  で暗号化し共通鍵  $K_t$  をサービスプロバイダ (SP) の公開鍵で暗号化する。

6) テンプレートを個人識別認証局 (IDA) の公開鍵で暗号化する。

7) テンプレートを共通鍵  $K_t$  で暗号化し共通鍵  $K_t$  を個人識別認証局 (IDA) の公開鍵で暗号化する。

#### 【0072】

上記7種類の態様があるが、これらの処理について図6、図7、図8を用いて説明する。図6(a)は、テンプレートを暗号化しない場合の処理であり、個人識別装置から取得した例えば指紋等の生体情報をテンプレート、具体的には指紋データをコード化したデータをそのままテンプレート情報として、個人識別証明書 (IDC) に格納する。

#### 【0073】

図6(b)は、公開鍵のみを使用した暗号化、復号処理を示す図であり、(b-1)の暗号化処理においては、個人識別装置から取得したユーザの識別情報であるテンプレートを、そのユーザまたはユーザデバイスの公開鍵、サービスプロバイダ (SP) (個人識別証明書を利用してサービス提供ユーザの識別を実行する SP) の公開鍵、または、個人識別認証局 (IDA) の公開鍵のいずれかを用いて暗号化する。暗号化方式は例えば楕円曲線暗号 (Elliptic Curve Cryptography (ECC))、RSA暗号 (Rivest, Shamir, Adleman) が適用される。暗号化されたテンプレートは、そのテンプレートの暗号化処理に適用した暗号方式 (アルゴリズム) と、公開鍵の識別子 (固有 ID) とともに個人識別証明書 (IDC) に格納される。

#### 【0074】

なお、ここで使用される公開鍵は、公開鍵固有 ID によって識別可能な公開鍵

である。公開鍵固有 I D は公開鍵証明書を特定可能な情報であり、例えば公開鍵証明書に格納されたユーザ I D、ユーザ名等が使用可能である。使用する公開鍵は、ユーザの公開鍵、サービスプロバイダ（S P）（個人識別証明書を利用してサービス提供ユーザの識別を実行する S P）の公開鍵、または、個人識別認証局（I D A）の公開鍵のいずれかであり、個人識別証明書（I D C）の使用形態によって選択される。

## 【 0 0 7 5 】

図 7 にテンプレートの暗号化に使用する公開鍵の使用形態の場合分けについて説明する図を示す。例えば、ユーザまたはユーザデバイスの公開鍵をテンプレート暗号化に用いる個人識別証明書（I D C）の使用例には、ユーザデバイス（例えば P C）の使用許可を付与した特定ユーザの識別を行なうために使用する個人識別証明書（I D C）がある。P C 使用の際に、個人識別証明書（I D C）の格納テンプレートをユーザ秘密鍵で復号し、復号によって得られたテンプレートと入力テンプレートの比較により、各ユーザの個人識別を行なう場合等である。

## 【 0 0 7 6 】

サービスプロバイダの公開鍵をテンプレート暗号化に用いる個人識別証明書（I D C）の使用例としては、サービスプロバイダにおいて特定ユーザ、例えば、サービスを提供するユーザを識別するための個人識別証明書（I D C）がある。サービスプロバイダは、サービスプロバイダが保有、あるいはユーザまたは個人識別認証局（I D A）から送付される各ユーザの個人識別証明書（I D C）から暗号化テンプレート情報を取り出してサービスプロバイダの秘密鍵を用いて復号し、認証処理の対象となる個人の提出したサンプリング情報（指紋データ等）と復号したテンプレートとの照合処理を実行する。

## 【 0 0 7 7 】

個人識別認証局の公開鍵をテンプレート暗号化に用いる個人識別証明書（I D C）の使用例としては、例えば、端末間でのデータ送受信を実行するデータ送受信者において、個人識別認証局（I D A）発行の個人識別証明書（I D C）を用いて個人識別処理を行なう場合がある。このように、個人識別証明書（I D C）の使用形態に応じて、I D C 内に格納するテンプレート情報の暗号化形態が異な

ってくる。

【0078】

図6、(b-2)は、公開鍵暗号方式で暗号化されたテンプレートの復号処理を示す図であり、個人識別証明書(IDC)から、暗号化テンプレートを取り出して、さらに、暗号方式、公開鍵固有IDを取り出す。さらに、公開鍵固有IDから特定される公開鍵に対応する秘密鍵を取り出して、取り出した秘密鍵により、暗号化テンプレートの復号処理を実行して、テンプレートを取り出す。個人名認証を実行するユーザデバイスあるいはサービスプロバイダ等の個人認証実行エンティティは、これらのデータ復号、暗号処理を実行可能な暗号処理部を有する。

【0079】

図8は、共通鍵と公開鍵とを使用したテンプレート暗号化処理、復号処理を説明する図である。(c-1)は、暗号化処理のプロセスを説明したものであり、まず、暗号化テンプレート情報を生成しようとする例えば個人識別認証局(IDA)において、乱数から共通鍵を生成し、個人識別装置から入力されたテンプレートに対して、共通鍵で暗号化を実行する。さらに、そのユーザまたはユーザデバイスの公開鍵、サービスプロバイダ(SP)の公開鍵、または、個人識別認証局(IDA)の公開鍵のいずれか適用する公開鍵を共通鍵を用いて暗号化する。これらの公開鍵の選択は、前述した図7の使用態様に応じて行なうものである。

【0080】

このようにして生成された暗号化テンプレートおよび暗号化共通鍵を、テンプレート暗号化、共通鍵暗号化に適用した暗号方式(アルゴリズム)と、公開鍵の識別子(固有ID)とともに個人識別証明書(IDC)に格納する。

【0081】

(c-2)は、共通鍵と秘密鍵とを使用した復号処理を示す図であり、個人識別証明書(IDC)の暗号化テンプレート情報から、暗号化テンプレートを取り出して、さらに、暗号化された共通鍵、暗号方式、公開鍵固有IDを取り出す。さらに、公開鍵固有IDから特定される公開鍵により特定される秘密鍵を用いて暗号化共通鍵の復号を実行し、復号して得られる共通鍵に基づいて、暗号化テン

プレートの復号処理を実行して、テンプレートを取り出す。

【0082】

### 〔3. テンプレート、個人識別証明書（IDC）の登録、変更処理〕

次に上述したデータ内容を持つ個人識別証明書（IDC）の登録、削除、変更、追加、停止、停止解除処理について説明する。なお、停止は、IDCの有効性を一旦停止する処理であり、停止解除処理は、一旦、有効性が停止されたIDCを再度有効にする処理である。

【0083】

#### （3. 1. テンプレート登録）

個人識別証明書（IDC）を有効に登録するには、まず、個人識別証明書（IDC）の証明対象となる個人がサンプリング情報を提供してテンプレートを登録することが必要となる。テンプレートは、前述したように、個人の生体（バイオメトリクス）情報、例えば指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報、生体情報以外の個人識別情報、例えば印鑑、パスポート、免許書、カード等の識別データ、あるいは、上記各情報の組合わせ、または、上記各情報とパスワードとの組み合わせ等、基本的に本人のみが持ち得る情報を含む情報である。

【0084】

テンプレート登録、IDC生成処理の流れを図9に示す。テンプレートの登録処理は、上記各種の態様の個人情報を探取可能な装置を用いて採取された情報（サンプリング情報）に基づいて行なう。例えば指紋情報をテンプレートとして用いる場合は指紋読み取り装置、声紋情報を使用する場合は、声紋情報の取得装置を用いて採取する（S11）。取得データは、オンラインまたはオフラインにより個人識別認証局（IDA）に送られる（S12）。また、ユーザは個人情報（PIN）を本人確認のために個人識別認証局（IDA）に送る（S13）。

【0085】

これらのデータがオンラインで送られる場合は、ユーザのデバイスと個人識別認証局（IDA）間での相互認証処理が実行され、転送データには電子署名が付加され、データ受信側では署名検証が実行される。個人識別認証局（IDA）はデータの改竄チェックを実行し、本人確認を実行し、データ正当性の検証を行な

う（S 1 4）。正当性が確認されない場合はエラー（S 1 7）として登録処理は実行されない。

#### 【 0 0 8 6 】

個人識別認証局（I D A）は、テンプレートの登録に際して、本人確認可能な個人証明データにより本人確認処理を実行する。また、必要に応じて住所、連絡先等の個人情報を取得する。個人識別認証局（I D A）は、本人確認および必要データの確認の後、テンプレートに個人識別子を割り当て、データベースに格納（S 1 5）し、テンプレートを個人識別認証局（I D A）の公開鍵で暗号化して、暗号化テンプレートを格納した個人識別証明書（I D C）を生成する（S 1 6）。なお、I D Cにおけるテンプレートの暗号化鍵は、I D Cの使用場所、すなわち個人認証実行エンティティに応じて異なって使用される場合があり、例えばサービスプロバイダ、またはユーザデバイス等の公開鍵を用いて行われることもある。

#### 【 0 0 8 7 】

##### （ 3 . 2 . テンプレート削除）

個人識別認証局（I D A）に登録したテンプレートは、テンプレート削除処理により、削除可能である。削除処理は、例えば、ユーザからの削除要求により実行される。テンプレート削除処理の流れを図 1 0 に示す。ユーザは、削除要求（S 2 1）にともない、ユーザ身元の確認可能な個人証明データを個人識別認証局（I D A）に提出する（S 2 2）。ユーザは、さらに個人情報（P I N）を本人確認のために個人識別認証局（I D A）に送る（S 2 3）。

#### 【 0 0 8 8 】

これらのデータがオンラインで送られる場合は、ユーザのデバイスと個人識別認証局（I D A）間での相互認証処理が実行され、転送データには電子署名が付加され、データ受信側では署名検証が実行される。個人識別認証局（I D A）はデータの改竄チェックを実行し、本人確認を実行し、データ正当性の検証を行なう（S 2 4）。正当性が確認されない場合はエラー（S 2 7）として削除処理は実行されない。

#### 【 0 0 8 9 】

個人識別認証局（IDA）は、ユーザ身元の確認を個人証明データにより行い、本人からの要求であることを確認（S24）して、削除要求対象のテンプレート、個人識別データ、その他、付加情報の削除を実行する（S25）。さらに、テンプレートの格納された個人識別証明書（IDC）の削除を行ない、削除されたIDCを失効リストに登録する（S26）。具体的には、失効リストに対して対応するIDC識別子を登録する。

## 【0090】

## （3. 3. テンプレート変更）

個人識別認証局（IDA）に登録したテンプレートは、テンプレート変更処理により、変更可能である。テンプレート変更処理の流れを図11に示す。ユーザは、個人識別認証局（IDA）に対してテンプレート変更要求を提出（S31）し、新たなテンプレート生成用のサンプリング情報等を採取し（S32）、さらに、身元確認のための個人証明データ、付加情報（PIN）を必要に応じて個人識別認証局（IDA）に送付する（S33, S34）。個人識別認証局（IDA）は、個人証明データに基づいて個人確認を実行（S35）し、変更前のテンプレートに基づく個人識別証明書（IDC）を削除（S36）し、失効リストに登録（S37）する。さらに、新たなテンプレートに識別番号を付与してデータベースに格納（S38）し、テンプレートを個人識別認証局（IDA）の公開鍵で暗号化して、暗号化テンプレートを格納した個人識別証明書（IDC）を生成（S39）する。なお、ユーザデバイスと個人識別認証局（IDA）との間のオンラインでのデータ通信においては、前述の処理と同様、相互認証処理、通信データの署名付加、検証処理を実行する。

## 【0091】

## （3. 4. テンプレート追加）

ユーザは、個人識別認証局（IDA）に登録したテンプレートに、さらに別の個人識別データを追加テンプレートとして追加することができる。テンプレート追加処理の流れを図12に示す。ユーザは、テンプレート追加要求を個人識別認証局（IDA）に実行（S41）し、新たなテンプレートを採取装置により採取（S42）し、個人識別認証局（IDA）に対して個人証明データとともに送付



(S 4 3, S 4 4) する。個人識別認証局 (I D A) は、受領した個人証明データの検証 (S 4 5) により、本人確認を実行して、追加テンプレートに対して個人識別子 (番号) を割り当ててデータベースに格納 (S 4 6) し、追加テンプレートを個人識別認証局 (I D A) の公開鍵で暗号化して、暗号化テンプレートを格納した個人識別証明書 (I D C) を生成 (S 4 7) する。なお、ユーザデバイスと個人識別認証局 (I D A) との間のオンラインでのデータ通信においては、前述の処理と同様、相互認証処理、通信データの署名付加、検証処理を実行する。

#### 【 0 0 9 2 】

##### ( 3 . 5 . テンプレート停止 )

個人識別認証局 (I D A) に登録したテンプレートを一次的に使用を停止する処理がユーザからの停止要求により実行できる。テンプレート停止処理の流れを図 1 3 に示す。ユーザは、テンプレート停止要求を個人識別認証局 (I D A) に実行 (S 5 1) し、ユーザは、個人証明データ、付加情報を個人識別認証局 (I D A) に提出する (S 5 2, S 5 3) と、個人識別認証局 (I D A) は、個人証明データにより本人確認を行ない (S 5 4)、要求のあったユーザのテンプレート、個人証明データ、付加情報の有効性を停止 (S 5 5) する。この停止処理の際に、個人識別認証局 (I D A) は、ユーザの個人識別証明書 (I D C) の失効処理、失効リスト登録 (S 5 6) を行なう。具体的には、失効リストに対して対応する I D C 識別子を登録する。なお、ユーザデバイスと個人識別認証局 (I D A) との間のオンラインでのデータ通信においては、前述の処理と同様、相互認証処理、通信データの署名付加、検証処理を実行する。

#### 【 0 0 9 3 】

##### ( 3 . 6 . テンプレート停止解除 )

停止処理により、有効性の停止されたテンプレートは、ユーザからの停止解除要求により、有効性を回復することができる。テンプレート停止解除処理の流れを図 1 4 に示す。ユーザは、テンプレート停止解除要求を個人識別認証局 (I D A) に実行 (S 6 1) し、ユーザは、個人証明データ、必要な付加情報を個人識別認証局 (I D A) に提出する (S 6 2, S 6 3)。個人識別認証局 (I D A)

は個人証明データによる本人確認（S64）の後、要求のあったユーザのテンプレート、個人証明データ、付加情報の有効性の停止解除を行なう（S65）。さらに、個人識別認証局（IDA）は、ユーザの個人識別証明書（IDC）が登録された失効リストの更新を行なう（S66）。具体的には、失効リストから対応するIDC識別子を削除する。なお、ユーザデバイスと個人識別認証局（IDA）との間のオンラインでのデータ通信においては、前述の処理と同様、相互認証処理、通信データの署名付加、検証処理を実行する。

【0094】

### （3. 7. 個人識別証明書（IDC）配布）

次に、ユーザから提供され、登録されたテンプレートに基づいて生成される個人識別証明書（IDC）配布処理について説明する。

【0095】

図15にサービスプロバイダ（SP）に対する個人識別証明書（IDC）配布処理の流れを示す。まず、個人識別証明書（IDC）を利用しようとするサービスプロバイダは、個人識別認証局（IDA）との間で、個人識別証明書（IDC）の利用に関する運用規程を含む契約を行なう（S71）。その後、個人識別認証局（IDA）とサービスプロバイダ（SP）間での相互認証処理（S72）を行なう。相互認証処理は、例えば共通鍵暗号方式、または公開鍵暗号方式に基づく処理として実行される。

【0096】

相互認証処理が成立すると、サービスプロバイダ（SP）は、SPのサービス提供予定のユーザ名あるいはユーザ識別データと、必要とする個人識別証明書（IDC）のポリシーを個人識別証明書（IDC）発行要求として個人識別認証局（IDA）に送付する（S73）。個人識別認証局（IDA）は、発行要求を検証（S74）し、運用規程に従って、個人識別証明書（IDC）のポリシーを設定（S75）し、要求のあったユーザの個人識別証明書（IDC）をデータベースから抽出し、個人識別認証局（IDA）の公開鍵で暗号化されているユーザ・テンプレートを復号した後、サービスプロバイダ（SP）の公開鍵で再暗号化（S76）して、設定ポリシーに基づく個人識別証明書（IDC）を生成（S77）

）して、生成 IDC をサービスプロバイダ（SP）に提供する（S78）。なお、データベースに格納されたテンプレートが暗号化されていない場合、暗号化の要請がない場合は、テンプレートの暗号化処理は省略可能である。

#### 【0097】

#### （3.8. 個人識別証明書（IDC）更新）

次に、ユーザから提供され、登録されたテンプレートに基づいて生成される個人識別証明書（IDC）の更新処理について説明する。更新処理は、主に使用している個人識別証明書（IDC）に設定された有効期限の再設定処理として実行される。

#### 【0098】

図16にサービスプロバイダ（SP）からの個人識別証明書（IDC）更新要求に対する処理の流れを示す。まず、個人識別証明書（IDC）を利用しようとするサービスプロバイダは、個人識別認証局（IDA）との間で、個人識別証明書（IDC）の利用に関する運用規程を含む契約を行なう（S81）。その後、個人識別認証局（IDA）とサービスプロバイダ（SP）間での相互認証処理を行なう（S82）。相互認証処理は、例えば共通鍵暗号方式、または公開鍵暗号方式に基づく処理として実行される。

#### 【0099】

相互認証処理が成立すると、サービスプロバイダ（SP）は、更新を必要とする個人識別証明書（IDC）の更新要求を個人識別認証局（IDA）に送付（S83）する。個人識別認証局（IDA）は、更新要求を検証（S84）し、運用規程に従って、個人識別証明書（IDC）のポリシーを設定（S85）し、要求のあったユーザの個人識別証明書（IDC）をデータベースから抽出し、個人識別認証局（IDA）の公開鍵で暗号化されているユーザ・テンプレートを復号した後、サービスプロバイダ（SP）の公開鍵で再暗号化して、設定ポリシーに基づく個人識別証明書（IDC）を生成（S86）して、有効期間の設定を行ない、生成 IDC をサービスプロバイダ（SP）に提供（S87）する。なお、データベースに格納されたテンプレートが暗号化されていない場合、暗号化の要請がない場合は、テンプレートの暗号化処理は省略可能である。

## 【0100】

## (3. 9. 個人識別証明書 (IDC) 削除)

次に、ユーザから提供され、登録されたテンプレートに基づいて生成される個人識別証明書 (IDC) の削除処理について説明する。

## 【0101】

図17にユーザからの個人識別証明書 (IDC) 削除要求に対する処理の流れを示す。まず、個人識別証明書 (IDC) を削除しようとするユーザは、削除を必要とする個人識別証明書 (IDC) の削除要求を個人識別認証局 (IDA) に送付 (S91) する。個人識別認証局 (IDA) は、削除要求を検証 (S92) し、対応する個人識別証明書 (IDC) の削除を実行 (S93) する。

## 【0102】

## (3. 10. 個人識別証明書 (IDC) 照会)

次に、ユーザから提供され、登録されたテンプレートに基づいて生成される個人識別証明書 (IDC) の照会処理について説明する。照会処理は、例えばサービスプロバイダ (SP) が個人識別証明書 (IDC) を保有せず、ユーザから送付されたサンプリングデータを個人識別認証局 (IDA) に送付して、個人識別認証局 (IDA) にのにおいて、個人識別認証局 (IDA) が保有する個人識別証明書 (IDC) に基づいて個人認証を行なって、その結果のみをサービスプロバイダ (SP) が利用するような場合に実行される処理である。

## 【0103】

図18にサービスプロバイダ (SP) からの個人識別証明書 (IDC) 照会要求に対する処理の流れを示す。まず、個人識別証明書 (IDC) の照会を行なおうとするサービスプロバイダは、個人識別認証局 (IDA) との間で、個人識別証明書 (IDC) の利用に関する運用規程を含む契約を行なう (S01)。その後、個人識別認証局 (IDA) とサービスプロバイダ (SP) 間での相互認証処理を行なう (S02)。相互認証処理は、例えば共通鍵暗号方式、または公開鍵暗号方式に基づく処理として実行される。

## 【0104】

相互認証処理が成立すると、サービスプロバイダ (SP) は、照会を必要とす

る個人識別証明書（IDC）の照会要求を個人識別認証局（IDA）に送付するとともに、照会ユーザのサンプリングデータ等を送付（S03，S04）する。個人識別認証局（IDA）は、照会要求を検証（S05）し、受領サンプリングデータと個人識別証明書（IDC）との照合（S06）を行い、照合結果（OKまたはNG）をサービスプロバイダ（SP）に送付（S07）する。

## 【0105】

## [4. 個人識別証明書（IDC）の基本的利用形態]

以下、個人識別証明書（IDC）の基本的利用形態について、公開鍵証明書（PKC）を発行する認証局（CA）と、個人識別証明書（IDC）を発行する個人識別認証局（IDA）と、これら各証明書を利用するデバイスとの関係を中心として説明する。

## 【0106】

図19および図20に公開鍵証明書（PKC）を発行する認証局（CA）と、個人識別証明書（IDC）を発行する個人識別認証局（IDA）と、これら各証明書を利用するデバイスの2つの構成例を示す。図19の構成は、個人識別証明書（IDC）のテンプレートとサンプリング情報との比較を個人識別認証局（IDA）において実行する形態、図20は、個人識別証明書（IDC）のテンプレートとサンプリング情報との比較をサービスプロバイダ（SP）またはユーザデバイス（UD）において実行する形態における各システム構成を示している。

## 【0107】

図19のユーザデバイス（UD）またはサービスプロバイダ（SP）300は、指紋データ等の様々な個人情報を取得し、処理するためのサンプリング情報処理部310を有し、サンプリング情報処理部310は、サンプリング情報を取得するための個人情報取得部314、指紋データ等のコード変換処理等を実行する情報変換部313、これらの変換コードを個人識別認証局320に送信する通信部312を有し、また、各種通信処理において暗号データ処理に使用する公開鍵証明書を格納している。制御部311は、個人情報取得部314、情報変換部313、通信部312における処理の制御を実行する。

## 【0108】

個人識別認証局（IDA）320は、比較部321、記憶手段322を有し、比較部において記憶手段に格納された認証対象の各個人のテンプレート（個人識別証明書に格納され、暗号化されていることが望ましい）と、ユーザデバイス（UD）またはサービスプロバイダ（SP）300から受信するサンプリング情報との比較（照合）を実行する。記憶手段には、テンプレートの他に個人識別証明書の発行履歴、照合処理履歴データが格納される。

## 【0109】

認証局（CA）330は、公開鍵証明書（PKC）の発行機関であり、ユーザのリクエストに応じて、認証局の署名を付加したユーザの公開鍵証明書を発行する。認証局は、公開鍵証明書の発行履歴、照合処理履歴データを格納し、管理する。

## 【0110】

個人識別認証局（IDA）320は、ユーザデバイス（UD）またはサービスプロバイダ（SP）300からサンプリング情報を受信し、格納テンプレートとの比較を実行して、一致した場合には、結果通知としてOKまたはNGをユーザデバイス（UD）またはサービスプロバイダ（SP）300に通知する。また、後述するが、所定のフォーマットに従った照合証明書を発行する構成としてもよい。個人識別認証局は、照合証明書を発行した場合は、発行履歴を格納する。

## 【0111】

認証局、（CA）、個人識別認証局（IDA）320と、ユーザデバイス（UD）またはサービスプロバイダ（SP）300との間の通信は、相互認証処理の成立を条件として実行され、機密データに関しては、相互認証において生成したセッションキーによる暗号化、あるいは、双方の公開鍵による暗号化を施して実行するのが望ましい。

## 【0112】

図20は、個人識別証明書（IDC）のテンプレートとサンプリング情報との比較をサービスプロバイダ（SP）またはユーザデバイス（UD）において実行する形態におけるシステム構成例である。

## 【0113】

図20のユーザデバイス（UD）またはサービスプロバイダ（SP）400は、指紋データ等の様々な個人情報を取得し、さらに照合処理を実行するための照合システム410を有し、照合システム410は、個人識別証明書を格納した一般メモリ413、個人識別証明書の改竄チェック処理を実行する個人識別証明書検証部414、個人識別証明書に格納された暗号化テンプレートの復号処理を実行するテンプレート復号化部415、指紋データ等のサンプリング情報を取得するための個人情報取得部418、指紋データ等のコード変換処理等を実行する情報変換部417、復号したテンプレートとコード化されたサンプリング情報とを比較する比較部416、個人識別認証局420とのデータ通信を実行する通信部411を有し、また、各種通信処理において暗号データ処理のための署名生成部、公開鍵証明書、秘密鍵を持つ暗号処理部419を有している。制御部412は、各処理部における処理制御を実行する。

#### 【0114】

個人識別認証局（IDA）420は、個人識別証明書発行部421、記憶手段422を有し、認証対象の各個人のテンプレートを格納した個人識別証明書をユーザデバイス（UD）またはサービスプロバイダ（SP）400からのリクエストに応じて発行する。記憶手段422には、テンプレート、個人識別証明書、個人識別証明書の発行履歴、照合処理履歴データが格納される。

#### 【0115】

認証局（CA）430は、公開鍵証明書（PKC）の発行機関であり、ユーザのリクエストに応じて、認証局の署名を付加したユーザの公開鍵証明書を発行する。認証局は、公開鍵証明書の発行履歴、照合処理履歴データを格納し、管理する。

#### 【0116】

図19の構成と同様、認証局、（CA）、個人識別認証局（IDA）320と、ユーザデバイス（UD）またはサービスプロバイダ（SP）300との間の通信は、相互認証処理の成立を条件として実行され、機密データに関しては、相互認証において生成したセッションキーによる暗号化、あるいは、双方の公開鍵による暗号化を施して実行するのが望ましい。

【 0 1 1 7 】

〔 5. 個人識別証明書（ I D C ）を使用した認証処理態様〕

次に、上述の個人識別証明書（ I D C ）を用いた個人認証処理の様々な態様について説明する。個人識別証明書（ I D C ）を用いた個人認証処理は、下記の 2 つのモードに大別される。

【 0 1 1 8 】

（ 5. 1. オンラインモード）

静的照合(Static IDC verification)

個人識別証明書（ I D C ）のテンプレートは照合される場所、例えば個人識別認証局（ I D A ）、サービスプロバイダ（ S P ）、あるいはユーザデバイス（ P C ）の公開鍵で暗号化されて個人識別認証局（ I D A ）に登録、格納しており、サービスプロバイダ（ S P ）、あるいはユーザデバイス（ P C ）からの要求に応じて個人識別認証局（ I D A ）が I D C を配布し、照合処理を実行する。

【 0 1 1 9 】

動的照合(Dynamic IDC verification)

個人識別証明書（ I D C ）のテンプレートは個人識別認証局（ I D A ）の公開鍵で暗号化されて I D A に登録されており、サービスプロバイダ（ S P ）、あるいはユーザデバイス（ P C ）からの要求に応じて照合される場所、すなわち個人認証処理実行エンティティである例えば S P 、あるいは P C の公開鍵で暗号化し直し、動的に個人識別証明書（ I D C ）を配布し照合処理が実行される。

【 0 1 2 0 】

（ 5. 2. オフラインモード）

静的照合

個人識別証明書（ I D C ）のテンプレートは照合される場所、すなわち個人認証処理実行エンティティである例えば個人識別認証局（ I D A ）、サービスプロバイダ（ S P ）、あるいはユーザデバイス（ P C ）の公開鍵で暗号化、あるいは、テンプレートを共通鍵で暗号化し、該共通鍵を個人識別認証局（ I D A ）、サービスプロバイダ（ S P ）、あるいはユーザデバイス（ P C ）の公開鍵で暗号化して個人識別認証局（ I D A ）に登録され、各ユーザに配布されている。個人認



証する際、照合先にIDCとサンプリング情報を送り照合する。以下、上記の各モードにおける照合処理について説明する。

#### 【0121】

##### (5. 1. 1. オンラインモード静的照合)

オンラインモード静的照合は、個人識別証明書（IDC）のテンプレートと、各個人が入力したサンプリングデータとの照合処理の実行時に、個人識別認証局（IDA）が動的に個人識別証明書（IDC）を発行して、ユーザデバイス（PC）、サービスプロバイダ（SP）、個人識別認証局（IDA）のいずれかのシステムにおいて照合処理を実行する形態であり、個人識別証明書（IDC）のテンプレートと、各個人が入力したサンプリングデータとの照合処理を各システム、すなわち個人認証処理実行エンティティにおいて実行する形態であり、個人識別認証局（IDA）は、照合処理を実行するシステムの公開鍵で暗号化されたテンプレート情報をデータベースから抽出して各システムに送付し、各システムにおいて受信IDCを復号して得られるテンプレートと、入力サンプリングデータとの照合を実行して個人識別を行なう構成である。

#### 【0122】

図21にユーザデバイス（例えばPC）、サービスプロバイダ（SP）、個人識別認証局（IDA）の各システムにおける照合処理の実行形態を説明する図を示す。なお、図21（a）～（c）におけるユーザデバイス、サービスプロバイダ（SP）、個人識別認証局（IDA）等の各システム間におけるデータ転送は、基本的に各データ送受信システム間における相互認証処理が実行され、認証が成立したことを条件とし、認証処理において生成したセッションキーでデータの暗号化処理がなされて実行されるものである。

#### 【0123】

図21（a）は、ユーザデバイスにおいて照合処理を実行する形態である。個人識別認証局（IDA）には、ユーザデバイスの公開鍵で暗号化されたテンプレートを格納した個人識別証明書（IDC）が保管され、ユーザデバイスにおける照合処理の際には、ユーザデバイスから個人識別認証局（IDA）に対して、個人認証の対象となる個人の個人識別証明書（IDC）の取得要求を行なう。

## 【0124】

個人識別証明書（IDC）の取得は、例えばその認証対象である個人またはユーザデバイスの公開鍵証明書（PKC）の固有IDを、ユーザデバイスから個人識別認証局（IDA）に送信し、個人識別認証局（IDA）が受信した固有IDに基づいて格納IDC中から対応する個人のIDCを抽出してユーザデバイスに送信することにより実行される。公開鍵証明書（PKC）と個人識別証明書（IDC）とは、様々な態様のリンク構成が設定可能であり、設定されたリンク構成に応じたIDC識別データがユーザデバイスから個人識別認証局（IDA）に送付され、個人識別認証局（IDA）では、受信データをキーとして対応する個人識別証明書（IDC）の抽出処理を実行する。なお、公開鍵証明書（PKC）と個人識別証明書（IDC）とのリンク態様については後段で詳細に説明する。

## 【0125】

ユーザデバイスは、個人識別認証局（IDA）から受信した個人識別証明書（IDC）中の暗号化テンプレートをユーザデバイスの秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得されたテンプレートに対応する個人データ、例えば指紋データ等のサンプリングデータとの照合を実行する。照合において一致すればOKであり、不一致であればNGとなる。IDCの格納テンプレートと、サンプリングデータとは対応する個人データ、すなわち指紋データであれば指紋データ、虹彩データであればいずれも虹彩データであることが必要である。なお、複数の異なる個人識別データをテンプレートとして個人識別証明書（IDC）に格納し、そのいずれかと入力サンプリングデータとが一致すれば照合成立とする構成としてもよい。

## 【0126】

照合の成立を条件として、例えばその後のユーザデバイスに設定された特定のアプリケーションプログラムを実行し、データベースへのアクセス許可、あるいはデータ更新許可、データ入力許可、その他のデータ処理を実行可能とする。照合が不成立の場合は、データ処理の実行を不許可とする。この構成は、個人認証処理要求エンティティおよび個人認証処理実行エンティティが、照合処理機能を備えたデータ処理装置としてのユーザデバイスである。

## 【0127】

図21(b)は、サービスプロバイダ(SP)において照合処理を実行する形態である。個人識別認証局(IDA)には、サービスプロバイダ(SP)の公開鍵で暗号化されたテンプレートを格納した個人識別証明書(IDC)が保管され、サービスプロバイダ(SP)における照合処理の際には、ユーザデバイスから認証の実行対象となる個人のサンプリング情報と、その個人の公開鍵証明書(PKC)が送信される。サービスプロバイダ(SP)がPKCを既に保有している場合は、PKCを特定するための識別データでもよい。なお、サンプリングデータは、相互認証で生成したセッションキーで暗号化されるか、あるいは、サービスプロバイダ(SP)の公開鍵により暗号化され、サービスプロバイダ(SP)においてのみ復号可能な暗号化データとして送付することが好ましい。本構成は、個人認証処理要求エンティティはユーザデバイスであり、個人認証処理実行エンティティは、該ユーザデバイスに対してサービスを提供するサービスプロバイダである。

## 【0128】

サービスプロバイダ(SP)は、個人またはユーザデバイスの公開鍵証明書(PKC)の固有IDを、ユーザデバイスから個人識別認証局(IDA)に送信し、個人識別認証局(IDA)に対して、個人認証の対象となる個人に対応する個人識別証明書(IDC)の取得要求を行なう。個人識別認証局(IDA)は受信した固有IDに基づいて格納IDC中から対応する個人のIDCを抽出してサービスプロバイダ(SP)に送信する。このIDCは、サービスプロバイダ(SP)の公開鍵で暗号化されたテンプレートを含むIDCである。

## 【0129】

サービスプロバイダ(SP)は、個人識別認証局(IDA)から受信した個人識別証明書(IDC)中の暗号化テンプレートをサービスプロバイダ(SP)の秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得され、ユーザデバイスから送信された暗号化サンプリングデータ、例えば指紋データ等の暗号化サンプリングデータを復号したデータとの照合を実行する。照合において一致すればOKであり、不一致であればNGとなる。照合結果(OKまた

はNG)は、ユーザデバイスに送信され、照合結果に応じて、その後の処理、例えばユーザデバイスからサービスプロバイダ(S P)に対するコンテンツの送付要求、あるいはデータ閲覧要求等のサービス実行の可否が決定される。

#### 【0130】

図21(c)は、個人識別認証局(I D A)において照合処理を実行する形態である。個人識別認証局(I D A)には、個人識別認証局(I D A)の公開鍵で暗号化されたテンプレートを格納した個人識別証明書(I D C)が保管され、個人識別認証局(I D A)における照合処理の際には、ユーザデバイスから認証の実行対象となる個人のサンプリング情報と、その個人またはユーザデバイスの公開鍵証明書(P K C)がサービスプロバイダ(S P)を経由して個人識別認証局(I D A)に送付される。個人識別認証局(I D A)がP K Cを既に保有している場合は、P K Cを特定するための識別データでもよい。なお、サンプリングデータは、個人識別認証局(I D A)の公開鍵により暗号化され、個人識別認証局(I D A)においてのみ復号可能な暗号化データとして送付することが好ましい。本構成は、個人認証処理要求エンティティはユーザデバイスまたはサービスプロバイダであり、個人認証処理実行エンティティは個人識別認証局である。

#### 【0131】

個人識別認証局(I D A)は、個人の公開鍵証明書(P K C)の固有I Dに基づいて格納I D C中から対応する個人のI D Cを抽出して個人識別証明書(I D C)中の暗号化テンプレートを個人識別認証局(I D A)の秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得され、ユーザデバイスからサービスプロバイダ(S P)を経由して送信された暗号化サンプリングデータ、例えば指紋データ等の暗号化サンプリングデータを復号したデータとの照合を実行する。照合において一致すればOKであり、不一致であればNGとなる。照合結果(OKまたはNG)は、サービスプロバイダ(S P)および、ユーザデバイスに送信され、照合結果に応じて、その後の処理、例えばユーザデバイスからサービスプロバイダ(S P)に対するコンテンツの送付要求、あるいはデータ閲覧要求等のサービス実行の可否が決定される。

#### 【0132】

## (5. 1. 2 オンラインモード動的照合)

オンラインモード動的照合は、個人識別証明書（IDC）のテンプレートと、各個人が入力したサンプリングデータとの照合処理の実行時に、個人識別認証局（IDA）が動的に個人識別証明書（IDC）を発行して、ユーザデバイス（PC）、サービスプロバイダ（SP）、個人識別認証局（IDA）のいずれかのシステムにおいて照合処理を実行する形態であり、個人識別認証局（IDA）の公開鍵で暗号化されたテンプレート情報を、個人識別認証局（IDA）において復号し、照合処理を実行する各システムの公開鍵で再暗号化した IDC を各照合処理システムに送信して、各システムにおいて復号して得られるテンプレートと、入力サンプリングデータとの照合を実行して個人識別を行なう構成である。

## 【0133】

図 22 は、ユーザデバイスにおいて照合処理を実行する形態である。個人識別認証局（IDA）には、個人識別認証局（IDA）の公開鍵で暗号化されたテンプレートを格納した個人識別証明書（IDC）が保管され、ユーザデバイスにおける照合処理の際には、ユーザデバイスから個人識別認証局（IDA）に対して、個人認証の対象となる個人の個人識別証明書（IDC）の取得要求を行なう。

## 【0134】

個人識別証明書（IDC）の取得は、例えばその認証対象である個人またはユーザデバイスの公開鍵証明書（PKC）、または、個人識別認証局（IDA）がすでにその個人またはユーザデバイスの公開鍵証明書（PKC）を保有している場合は、公開鍵証明書（PKC）の固有 ID を、ユーザデバイスから個人識別認証局（IDA）に送信し、個人識別認証局（IDA）が受信した固有 ID、または PKC から取得した固有 ID に基づいて格納 IDC 中から対応する個人の IDC を抽出する。

## 【0135】

個人識別認証局（IDA）は、抽出した IDC の暗号化テンプレートを個人識別認証局（IDA）の秘密鍵で復号し、さらに、ユーザデバイスの公開鍵で再暗号化を行ない、個人識別証明書（IDC）を再発行し、再発行 IDC をユーザデバイスに送信する。

## 【0136】

ユーザデバイスは、個人識別認証局（IDA）から受信した個人識別証明書（IDC）中の暗号化テンプレートをユーザデバイスの秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得されたテンプレートに対応する個人データ、例えば指紋データ等のサンプリングデータとの照合を実行する。照合において一致すればOKであり、不一致であればNGとなる。照合の成立を条件として、例えばその後のユーザデバイスに設定された特定のアプリケーションプログラムを実行し、データベースへのアクセス許可、あるいはデータ更新許可、データ入力許可、その他のデータ処理を実行可能とする。照合が不成立の場合は、データ処理の実行を不許可とする。

## 【0137】

図23は、サービスプロバイダ（SP）において照合処理を実行する形態である。個人識別認証局（IDA）には、個人識別認証局（IDA）の公開鍵で暗号化されたテンプレートを格納した個人識別証明書（IDC）が保管され、サービスプロバイダ（SP）における照合処理の際には、まず、サービスプロバイダ（SP）から個人識別認証局（IDA）に対して、サービスプロバイダ（SP）の公開鍵証明書（PKC）が送信される。個人識別認証局（IDA）がサービスプロバイダ（SP）のPKCを既に保有している場合は、PKCを特定するための識別データでもよい。

## 【0138】

次に、ユーザデバイスから認証の実行対象となる個人またはユーザデバイスの公開鍵証明書（PKC）がサービスプロバイダ（SP）経由で、個人識別認証局（IDA）に送信される。個人識別認証局（IDA）がユーザデバイスのPKCを既に保有している場合は、PKCを特定するための識別データでもよい。

## 【0139】

個人識別認証局（IDA）は受信した固有IDに基づいて格納IDC中から対応する個人のIDCを抽出して、抽出したIDCの暗号化テンプレートを個人識別認証局（IDA）の秘密鍵で復号し、さらに、サービスプロバイダ（SP）の公開鍵で再暗号化を行ない、個人識別証明書（IDC）を再発行し、再発行ID

Cをサービスプロバイダ（SP）に送信する。

【0140】

サービスプロバイダ（SP）は、個人識別認証局（IDA）から受信した個人識別証明書（IDC）中の暗号化テンプレートをサービスプロバイダ（SP）の秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得され、ユーザデバイスから送信された暗号化サンプリングデータ、例えば指紋データ等の暗号化サンプリングデータを復号したデータとの照合を実行する。照合において一致すればOKであり、不一致であればNGとなる。照合結果（OKまたはNG）は、ユーザデバイスに送信され、照合結果に応じて、その後の処理、例えばユーザデバイスからサービスプロバイダ（SP）に対するコンテンツの送付要求、あるいはデータ閲覧要求等のサービス実行の可否が決定される。

【0141】

（5. 2. オフラインモード）

オフラインモードでは、オンラインモードのように、サンプリング情報との照合時に、個人識別認証局（IDA）が動的に個人識別証明書（IDC）を発行する構成ではなく、静的照合のみである。したがって個人識別証明書（IDC）に含まれるテンプレート情報の暗号方式、照合場所等により個人認証の実現方法が異なる。またオフラインモードでは個人識別証明書（IDC）に含まれる暗号化テンプレートの復号を照合場所、例えばユーザデバイス、またはサービスプロバイダ（SP）で行なうため、ユーザデバイス、またはサービスプロバイダ（SP）において復号可能な暗号化を行なうことが必要である。

【0142】

オフラインでの静的照合の処理形態は以下のような場合に分類される。

（5. 2. 1）デバイスでの照合

a. 個人識別証明書（IDC）と公開鍵証明書（PKC）が同一デバイスに格納されたユーザデバイスの場合

b. 個人識別証明書（IDC）と公開鍵証明書（PKC）が同一デバイスに格納されていないユーザデバイスの場合

（5. 2. 2）サービスプロバイダでの照合

c. 個人識別証明書（IDC）のテンプレート情報がサービスプロバイダ（SP）の公開鍵で暗号化されている場合

d. 個人識別証明書（IDC）のテンプレート情報がユーザデバイスの公開鍵、または共通鍵で暗号化されている場合

以下にそれぞれについて説明する。

【0143】

（5. 2. 1）デバイスでの照合

a. IDCとPKCが同一デバイスに格納されたユーザデバイスの場合

IDCとPKCが同一デバイスに格納されたユーザデバイスとは、個人識別証明書（IDC）に含まれるテンプレートとサンプリング情報との照合処理を実行するユーザデバイスに、照合対象のユーザの個人識別証明書（IDC）と公開鍵証明書（PKC）が存在し、その公開鍵証明書（PKC）に含まれるデバイスの公開鍵によって個人識別証明書（IDC）内のテンプレート情報が暗号化され、個人識別証明書（IDC）から公開鍵証明書（PKC）を特定可能な態様である。照合時には、個人識別証明書（IDC）に含まれるテンプレートの暗号化方式、暗号鍵としての公開鍵を持つ公開鍵証明書（PKC）を識別し、識別された公開鍵に対応する秘密鍵を特定し、秘密鍵によりテンプレートを復号する。

【0144】

図24にIDCとPKCを格納したユーザデバイスにおける照合処理を説明する図を示す。ユーザデバイスは、サンプリング情報採取装置により採取された指紋情報等の個人データをサンプリング情報として入力し、さらに、ユーザデバイス内に格納された個人識別証明書（IDC）を取り出し、テンプレート暗号化方式等の情報からテンプレート暗号化に適用された公開鍵の格納された公開鍵証明書（PKC）を識別し、識別された公開鍵に対応する秘密鍵を特定する。秘密鍵は、ユーザデバイスの公開鍵、秘密鍵ペアの構成要素であり、ユーザデバイスのセキュアメモリに格納されているので、格納された秘密鍵により、個人識別証明書（IDC）の暗号化テンプレートを復号する。次いで、復号したテンプレートと、サンプリング情報との照合処理を実行する。

【0145】



照合の成立を条件として、例えばその後のユーザデバイスに設定された特定のアプリケーションプログラムを実行し、データベースへのアクセス許可、あるいはデータ更新許可、データ入力許可、その他のデータ処理を実行可能とする。照合が不成立の場合は、データ処理の実行を不許可とする。

## 【 0 1 4 6 】

b. 個人識別証明書（IDC）と公開鍵証明書（PKC）が同一デバイスに格納されていないユーザデバイスの場合

多数のユーザが使用するデバイス（共有型ユーザデバイス）においては、ユーザそれぞれの個人識別証明書（IDC）を格納することは困難である。このような場合、各ユーザの個人識別証明書（IDC）を各個人端末（ex. ICカード等のモバイル端末）からユーザデバイスに取り込み、取り込んだIDCに基づいて処理を行なうことになる。この処理形態は、さらに、以下の3つの態様に分類される。

（b-1）個人端末格納のIDCを共有型ユーザデバイスへ送信し照合

（b-2）個人端末において復号したテンプレート情報を共有型ユーザデバイスへ送信し照合

（b-3）個人端末側での照合処理

これらの処理について、以下説明する。

## 【 0 1 4 7 】

（b-1）個人端末格納のIDCを共有型ユーザデバイスへ送信し照合

図25に、例えばICカード等の個人端末に格納された個人識別証明書（IDC）を共有型ユーザデバイスへ送信して照合処理を実行する構成について説明する図を示す。

## 【 0 1 4 8 】

共有型ユーザデバイスを用い、該共有ユーザデバイスに格納したアプリケーションプログラムにより、各種のデータ処理を実行しようとするそれぞれのユーザは、例えばICカード等のモバイル端末を共有ユーザデバイスに装着する。ICカードには、個人識別認証局（IDA）が発行した個人識別証明書（IDC）が格納されている。本構成では、共有ユーザデバイスが個人認証処理実行エンティ

テイである。

【 0 1 4 9 】

ＩＣカード等のモバイル個人端末を共有ユーザデバイスに装着し、モバイル端末から個人識別証明書（ＩＤＣ）を共有ユーザデバイスに送信する。なお、ＩＤＣ送信に先立ち、モバイル端末と共有ユーザデバイスとの間での相互認証が実行され、ＩＤＣを相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。

【 0 1 5 0 】

モバイル端末から個人識別証明書（ＩＤＣ）を受信した共有ユーザデバイスは、ＩＤＣに付加されている個人識別認証局（ＩＤＡ）の署名を検証し、ＩＤＣの改竄のないことを確認し、ＯＫ（改竄なし）の場合は、ＩＤＣから暗号化テンプレート情報を取り出す。なお、この暗号化テンプレートは、共有ユーザデバイスの公開鍵、あるいは共通鍵で暗号化されている。共有ユーザデバイスの公開鍵で暗号化されている場合は、共有ユーザデバイスの秘密鍵を用いて復号可能である。

【 0 1 5 1 】

テンプレートが共通鍵で暗号化されている場合は、図 2 5 の点線枠で示す処理を個人端末側で実行する。テンプレートを暗号化した共通鍵は、個人端末の公開鍵で暗号化して個人識別証明書（ＩＤＣ）に格納されている。個人端末は、個人識別証明書（ＩＤＣ）から暗号化共通鍵を取り出して、これを自己の秘密鍵で復号して共通鍵を取り出し、これを共有ユーザデバイスに送信する。なお、共通鍵は、相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。または、ユーザデバイスの公開鍵で共通鍵を暗号化して送付する構成としてもよい。

【 0 1 5 2 】

共有ユーザデバイスは、自己の秘密鍵、または共通鍵を用いて暗号化テンプレートを復号し、サンプリング情報採取装置から入力されたサンプリング情報との照合を実行する。

【 0 1 5 3 】

(b-2) 個人端末において復号したテンプレート情報を共有型ユーザデバイスへ送信し照合

図 2 6 に、例えば IC カード等の個人端末に格納された個人識別証明書 (IDC) を復号した後、共有型ユーザデバイスへ送信して照合処理を実行する構成について説明する図を示す。

【 0 1 5 4 】

ユーザは、IC カード等のモバイル端末を共有ユーザデバイスに装着し、モバイル端末において復号した個人識別証明書 (IDC) を共有ユーザデバイスに送信する。IDC は、個々のユーザのモバイル端末に対応して設定された公開鍵で暗号化され、モバイル端末に対応して設定された秘密鍵で復号可能なテンプレート情報を含む構成である。IDC から抽出された暗号化テンプレート情報は、モバイル端末に対応して設定された秘密鍵により復号され、その後、ユーザデバイスに送信される。なお、テンプレート送信に先立ち、モバイル端末と共有ユーザデバイスとの間での相互認証を実行し、テンプレートを相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。または、ユーザデバイスの公開鍵でテンプレートを暗号化して送付する構成としてもよい。

【 0 1 5 5 】

モバイル端末からテンプレートを受信した共有ユーザデバイスは、テンプレート情報を取り出し、サンプリング情報採取装置から入力されたサンプリング情報との照合を実行する。

【 0 1 5 6 】

(b-3) 個人端末側での照合処理

図 2 7 に、例えば IC カード等の個人端末に格納された個人識別証明書 (IDC) を用いて個人端末側で照合処理を実行して、その結果のみを共有型ユーザデバイスへ送信する構成について説明する図を示す。

【 0 1 5 7 】

ユーザは、IC カード等のモバイル端末を共有ユーザデバイスに装着し、モバイル端末において個人識別証明書 (IDC) の暗号化テンプレートの復号を実行する。IDC は、個々のユーザのモバイル端末に対応して設定された公開鍵で暗

号化され、モバイル端末に対応して設定された秘密鍵で復号可能なテンプレート情報を含む構成である。IDCから抽出された暗号化テンプレート情報は、モバイル端末に対応して設定された秘密鍵により復号される。

【0158】

サンプリング情報は、サンプリング情報採取装置において採取され、その後、ユーザデバイスを介してICカード等の個人端末に送信される。なお、サンプリング情報転送に先立ち、モバイル端末と共有ユーザデバイスとの間での相互認証を実行し、サンプリング情報を相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。ユーザデバイスからサンプリング情報を受信した個人端末は、復号したテンプレートとサンプリング情報との照合を実行し、その結果をユーザデバイスに送信する。本構成では、モバイル端末であるICカードが個人認証処理実行エンティティである。

【0159】

(5.2.2) サービスプロバイダでの照合

次に、サービスプロバイダ(SP)における様々なサービス提供に際しての個人認証処理をサービスプロバイダにおいて実行する処理形態について説明する。

【0160】

c. 個人識別証明書(IDC)のテンプレート情報がサービスプロバイダ(SP)の公開鍵で暗号化されている場合

まず、個人識別証明書(IDC)のテンプレート情報がサービスプロバイダ(SP)の公開鍵で暗号化されている場合の処理について、図28を用いて説明する。

【0161】

サービスプロバイダ(SP)の提供するサービス、例えばコンテンツ配信、決済等のサービスを受けようとするユーザデバイスは、まず、サンプリング情報採取装置により個人の指紋データ等のサンプリング情報を取得する。次に、ユーザデバイスは、サービスプロバイダ(SP)との間で相互認証処理を実行し、認証成立を条件としてサンプリング情報をサービスプロバイダ(SP)に送信する。サンプリング情報は、相互認証時に生成したセッションキー、または、サービス

プロバイダの公開鍵による暗号化を施して送信する。さらに、ユーザデバイスは、自己の個人識別証明書（IDC）をサービスプロバイダに送信する。この個人識別証明書（IDC）には、サービスプロバイダの公開鍵による暗号化の施されたテンプレート情報が格納されている。

#### 【0162】

ユーザデバイスからサンプリング情報と、個人識別証明書（IDC）とを受信したサービスプロバイダ（SP）は、個人識別証明書（IDC）に格納された暗号化テンプレート情報を自己（SP）の秘密鍵を用いて復号し、これとサンプリング情報との照合処理を実行する。

#### 【0163】

照合が成立した場合は、個人認証が成立したとみなされ、そのサービスプロバイダの提供する例えばコンテンツ配信、決済処理等の各種サービスをユーザ（ユーザデバイス）に対して実行する。照合不成立である場合は、個人認証が不成立とみなされ、サービス提供の実行を停止する。

#### 【0164】

d. 個人識別証明書（IDC）のテンプレート情報がユーザデバイスの公開鍵、または共通鍵で暗号化されている場合

次に、個人識別証明書（IDC）のテンプレート情報がユーザデバイスの公開鍵、または共通鍵で暗号化されている場合のサービスプロバイダ（SP）における個人認証について説明する。この場合の処理形態は、以下の3形態に分類される。

（d-1）ユーザデバイスによりテンプレートの暗号化に使用した共通鍵をサービスプロバイダ（SP）に送信して照合する場合、

（d-2）ユーザデバイスにおいて復号したテンプレート情報をサービスプロバイダ（SP）に送信して照合する場合、

（d-3）ユーザデバイス側での照合処理

これらの処理について、以下説明する。

#### 【0165】

（d-1）ユーザデバイス格納のIDCを共有型ユーザデバイスへ送信し照合

図 2 9 に、ユーザデバイスに格納された個人識別証明書（IDC）をサービスプロバイダ（SP）へ送信して照合処理を実行する構成について説明する図を示す。

【0166】

サービスプロバイダ（SP）のサービスを受けようとするユーザデバイスのユーザは、まず、サービスプロバイダ（SP）との間で相互認証処理を実行し、認証成立を条件として自己の個人識別証明書（IDC）をサービスプロバイダに送信する。なお、IDCは相互認証時に生成したセッションキー、あるいはサービスプロバイダ（SP）の公開鍵で暗号化して送付する構成が望ましい。

【0167】

ユーザデバイスから個人識別証明書（IDC）を受信したサービスプロバイダ（SP）は、IDCに付加されている個人識別認証局（IDA）の署名を検証し、IDCの改竄のないことを確認し、OK（改竄なし）の場合は、IDCから暗号化テンプレート情報を取り出す。なお、この暗号化テンプレートは共通鍵で暗号化されている。

【0168】

テンプレートを暗号化した共通鍵は、ユーザデバイスの公開鍵で暗号化して個人識別証明書（IDC）に格納されている。ユーザデバイスは、個人識別証明書（IDC）から暗号化共通鍵を取り出して、これを自己の秘密鍵で復号して共通鍵を取り出し、これをサービスプロバイダ（SP）に送信する。なお、共通鍵は、相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。または、サービスプロバイダ（SP）の公開鍵で共通鍵を暗号化して送付する構成としてもよい。

【0169】

サービスプロバイダ（SP）は、自己の秘密鍵、またはセッションキーで復号して共通鍵を取得し、取得した共通鍵を用いて暗号化テンプレートを復号し、サンプリング情報採取装置から入力され、ユーザデバイスを介して送付されたサンプリング情報との照合を実行する。ユーザデバイスは、サービスプロバイダ（SP）との間で相互認証処理を実行し、認証成立を条件としてサンプリング情報を

サービスプロバイダ（ＳＰ）に送信する。サンプリング情報は、相互認証時に生成したセッションキー、または、サービスプロバイダの公開鍵による暗号化を施して送信する。

【 0 1 7 0 】

（ｄ－２）ユーザデバイスにおいて復号したテンプレート情報をサービスプロバイダ（ＳＰ）へ送信し照合

図 3 0 に、ユーザデバイスに格納された個人識別証明書（ＩＤＣ）を復号した後、サービスプロバイダ（ＳＰ）へ送信して照合処理を実行する構成について説明する図を示す。

【 0 1 7 1 】

ユーザは、ユーザデバイスにおいて復号した個人識別証明書（ＩＤＣ）をサービスプロバイダ（ＳＰ）に送信する。ＩＤＣは、個々のユーザデバイスに対応して設定された公開鍵で暗号化され、ユーザデバイスに対応して設定された秘密鍵で復号可能なテンプレート情報を含む構成である。ＩＤＣから抽出された暗号化テンプレート情報は、ユーザデバイスに対応して設定された秘密鍵により復号され、その後、サービスプロバイダ（ＳＰ）に送信される。なお、テンプレート送信に先立ち、ユーザデバイスとサービスプロバイダ（ＳＰ）との間での相互認証を実行し、テンプレートを相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。または、サービスプロバイダ（ＳＰ）の公開鍵でテンプレートを暗号化して送付する構成としてもよい。

【 0 1 7 2 】

ユーザデバイスからテンプレートを受信したサービスプロバイダ（ＳＰ）は、テンプレート情報を取り出し、サンプリング情報採取装置から入力され、ユーザデバイスを介して受信したサンプリング情報との照合を実行する。

【 0 1 7 3 】

（ｂ－３）ユーザデバイス側での照合処理

図 3 1 に、ユーザデバイスに格納された個人識別証明書（ＩＤＣ）を用いてユーザデバイス側で照合処理を実行して、その結果のみをサービスプロバイダ（ＳＰ）へ送信する構成について説明する図を示す。

## 【 0 1 7 4 】

ユーザデバイスは、個人識別証明書（IDC）の暗号化テンプレートの復号を実行する。IDCは、個々のユーザデバイスに対応して設定された公開鍵で暗号化され、ユーザデバイスに対応して設定された秘密鍵で復号可能なテンプレート情報を含む構成である。IDCから抽出された暗号化テンプレート情報は、ユーザデバイスに対応して設定された秘密鍵により復号される。

## 【 0 1 7 5 】

サンプリング情報は、サンプリング情報採取装置において採取され、その後、ユーザデバイスに入力されて、復号したテンプレートとサンプリング情報との照合を実行し、その結果をサービスプロバイダ（SP）に送信する。サービスプロバイダ（SP）は、結果に基づいてサービスの提供の可否を決定する。

## 【 0 1 7 6 】

〔 6. 個人識別証明書に基づくユーザ認証によるコンテンツの利用権制御処理〕

次に、音楽データ、画像データ、ゲーム等の各種プログラム等、様々なコンテンツの利用において、個人識別証明書（IDC）に基づいてユーザ認証を実行することにより、コンテンツ利用権を制御する処理構成について説明する。

## 【 0 1 7 7 】

図 3 2 にコンテンツ取り引きにおいて流通するコンテンツを含むセキュア・コンテナ（Secure Container）の構成を示す。サービスプロバイダからユーザデバイスに対するコンテンツ配信、さらに、ユーザデバイスから他のユーザデバイスに対するコンテンツ配信においても図 3 2 に示すセキュアコンテナを流通させる。

## 【 0 1 7 8 】

なお、セキュアコンテナは、サービスプロバイダからユーザに配信されるばかりでなく、ユーザ間配信が可能である。ユーザ間コンテンツ配信の形態にはさらに 2 つの形態がある。1 つは、ユーザ A からユーザ B、さらにユーザ B からユーザ C 等、直列的に異なるユーザ間をコンテンツが順次、取り引きされる形態である。この直列的なユーザ間のコンテンツ配信が「世代間配信」である。もう 1 つ



の配信形態は、ユーザ A の購入したコンテンツをユーザ A からユーザ B, C, D 等、並列的に配信する形態である。すなわち 1 人のユーザから複数のユーザに並列に同一コンテンツを配信する形態である。この並列的なコンテンツ配信が「二次配信」である。

## 【 0 1 7 9 】

図 3 2 に示すようにセキュアコンテナ 7 0 0 は、コンテンツ鍵によって暗号化されたコンテンツ 7 0 1 と、コンテンツの料金とコンテンツ料金の受け取り先、配分情報を含む価格情報 7 0 2 と、コンテンツの利用条件、例えば「世代間配信」「二次配信」等の転売が禁止されている 1 回限りの配信が許容されたコンテンツであるとか、複数回の転売が可能であるとか、複数回の転売が可能である場合の転売条件、例えば 2 回までの「世代間配信」と、3 回までの「二次配信」が許容されているコンテンツであるとか、あるいは利用可能期間等の設定情報としての販売条件 (UCP) 7 0 3 と、セキュアコンテナの作成者、例えばサービスプロバイダの電子署名 7 0 4 を含んで構成される。セキュアコンテナの価格情報 7 0 2、販売条件 (UCP) 7 0 3 をコンテナ情報と総称する。セキュアコンテナのコンテナ情報である価格情報 7 0 2、販売条件 (UCP) 7 0 3 の少なくともいずれか、あるいは両者にはコンテンツ利用の許可されたユーザの個人識別証明書 (IDC) のリストが含まれる。

## 【 0 1 8 0 】

図 3 3 に個人識別証明書 (IDC) のリスト構成を示す。個人識別証明書 (IDC) のリストには、ユーザの識別子であるユーザ ID、および各ユーザに対応する個人識別証明書 (IDC) の識別子がデータとして含まれる。

## 【 0 1 8 1 】

コンテナ情報である価格情報 7 0 2、販売条件 (UCP) 7 0 3 は、コンテンツ製作者、コンテンツプロバイダ、サービスプロバイダ等のいずれかが設定する管理データである。例えばサービスプロバイダは、予めユーザ登録をしているユーザの個人識別証明書 (IDC) のリストを価格情報 7 0 2、販売条件 7 0 3 等を含めて各データを生成する。電子署名は、コンテンツの流通を管理する機関による署名である。コンテンツの流通を管理する機関がサービスプロバイダであれ

ば、サービスプロバイダの署名となる。

#### 【 0 1 8 2 】

図 3 4 に販売条件 (UCP) 7 0 3 の具体的構成例を示す。図 3 4 に示すように販売条件 (UCP) には、コンテンツの利用可能なユーザの個人識別証明書 (IDC) の識別子をリスト化したデータである個人識別証明書 (IDC) リスト 7 1 1 を含む。さらに、コンテンツ識別子 (ID)、コンテンツの利用可能なユーザデバイスを設定した使用可能機器条件、コンテンツの利用可能な地域を設定した地域コード、どのようにコンテンツを利用してよいかを示す利用権タイプ (例えばコンテンツの再生可能回数、コンテンツの複製 (ダウンロード) 可能回数) が含まれる。

#### 【 0 1 8 3 】

利用権タイプは、コンテンツの利用権を設定したデータである。図 3 5 に利用権データの構成例を示す。ルール番号に対応付けて、利用権の内容、例えばコンテンツの再生権、複製 (コピー) 権、さらにそれぞれの権利期間、回数等が設定されている。なお、図中の SCMS はコピー回数等を設定したコピー制御情報である。ユーザは、セキュアコンテナの販売条件に設定されたルール番号により指定される利用権の範囲でコンテンツの再生、複製が許容される。

#### 【 0 1 8 4 】

さらに、図 3 4 に示す販売条件 (UCP) には、異なるユーザデバイス間での流通可能回数として、「世代間配信」の可能回数を設定した「UCP 世代管理情報」7 1 2 と、「二次配信」の可能回数を設定した「二次配信可能回数」7 1 3 が含まれている。「UCP 世代管理情報」に設定されたユーザ間配信可能回数は、セキュアコンテナの利用に応じてユーザデバイス内のメモリに格納される使用制御情報 (UCS : Usage Control Status) (図 3 8 参照) に引き継がれる。「UCP 世代管理情報」に設定されたユーザ間配信可能回数は、使用制御情報 (UCS) 中の「UCS 世代管理情報」、「UCS 二次配信可能回数」の元データとなり、「UCS 世代管理情報」、「UCS 二次配信可能回数」に基づいてコンテンツ処理の可否が決定される。「UCS 世代管理情報」はコンテンツの世代間配信毎に更新され、「UCS 二次配信可能回数」はコンテンツの二次配信毎に更新

される。使用制御情報（UCS : Usage Control Status）については後段で説明する。

【0185】

図36は、セキュアコンテナに含まれる価格情報のデータ構成例を示すものであり、図34の販売条件（UCP）と同様のコンテンツID等の情報の他に、価格情報ID、価格情報バージョンが含まれる。さらに、図34の販売条件（UCP）と同様、個人識別証明書（IDC）リスト721を含む。すなわちコンテンツの利用可能なユーザの個人識別証明書（IDC）の識別子をリスト化したデータを含む。

【0186】

図37にセキュアコンテナを利用したコンテンツの配信処理形態を示す。コンテンツプロバイダ（CP）801がセキュアコンテナに格納するコンテンツを生成、または取得し、コンテンツと、そのコンテンツの販売条件（UCP）データをコンテンツのユーザに対する配信を行なうサービスプロバイダ（SP）802に提供する。サービスプロバイダ（SP）802は、コンテンツの利用に対する価格情報を生成して、価格情報、販売条件（UCP）の少なくともいずれか、あるいは両者にコンテンツ利用の許可されたユーザの個人識別証明書（IDC）のリストを格納し、電子署名を行なってセキュアコンテナを形成し、ユーザデバイス803に送付する。

【0187】

ユーザデバイス803は、セキュアコンテナの署名検証を行なう。さらに、セキュアコンテナの各構成データである販売条件（UCP）データ、価格情報等の署名検証を行ない、各データの改竄チェックを実行し、さらに、販売条件（UCP）データ、価格情報のいずれかの個人識別証明書（IDC）リストから、自己のIDC識別子を抽出し、IDC識別子によって特定される個人識別証明書（IDC）を取得して、IDC内のテンプレートとサンプリング情報との照合を実行する。なお照合処理は、ユーザデバイス、サービスプロバイダ、個人識別認証局（IDA）のいずれかにおいて実行する。この個人認証の成立を条件として、コンテンツの利用、すなわちコンテンツの復号が実行可能となる。具体的には、照

合成立を条件としてコンテンツの暗号化に使用しているコンテンツ鍵をサービスプロバイダからユーザデバイスに送信する。ユーザデバイスは、コンテンツ鍵を利用してセキュアコンテナのコンテンツの復号、再生が可能となる。

**【 0 1 8 8 】**

ユーザデバイスは、さらに、セキュアコンテナをユーザデバイス 8 0 3 の記憶媒体に格納し、コンテンツ利用に際し発生する利用料金を課金情報として生成し、決済処理を行なうクリアリングセンタ 8 0 4 に送信する。課金情報は、前述の価格情報に設定されたデータに基づいて生成される。クリアリングセンタでは、課金情報に基づいて例えばユーザの電子マネー口座からの金額振替処理を実行する。ユーザデバイス 8 0 3 は、さらに他のユーザデバイス 8 0 5 に対してセキュアコンテナを流通させることができる。この態様については後述する。なお、ユーザデバイス 8 0 3、8 0 5 は、セキュアコンテナの格納に際し、使用制御情報 (UCS) を生成してメモリに格納する。

**【 0 1 8 9 】**

図 3 8 にセキュアコンテナ格納に応じてユーザデバイスにおいて生成されユーザデバイス内のメモリに格納される使用制御情報 (UCS : Usage Control Status) の例を示す。図 3 8 に示すように、使用制御情報 (UCS) には、コンテンツ ID、サービスプロバイダ ID 等の情報の他に、再生残り回数、複製残り回数等のコンテンツ利用の制限情報が含まれる。これら、再生残り回数、複製残り回数は、同一のユーザデバイス内で利用可能な再生残り回数、複製残り回数を示すデータである。これらは、コンテンツの販売条件 (UCP) データに含まれるコンテンツの利用権を設定した利用権データに基づいて生成され、更新、継承されるデータである。従って、ユーザデバイスは、コンテンツ利用権の設定情報であるコンテンツの販売条件 (UCP) データに含まれるコンテンツ利用権データ、あるいは利用権データに基づいて生成される使用制御情報に従ってコンテンツの利用を実行することになる。

**【 0 1 9 0 】**

使用制御情報 (UCS) には、さらに、個人識別証明書 (IDC) リスト 7 3 1 を含む。すなわちコンテンツの利用可能なユーザの個人識別証明書 (IDC)

の識別子をリスト化したデータを含む。このリストは、販売条件（UCP）に設定されたデータを継承したデータである。さらに、使用制御情報（UCS）には、「UCS 世代管理情報」732、および「UCS 二次配信可能回数」733が含まれる。

#### 【0191】

「UCS 世代管理情報」は前述したように、「世代間配信」の可能回数を設定したものであり、コンテンツを最初に購入したユーザデバイスは、販売条件（UCP）中の「UCP 世代管理情報」に一致する回数が設定され、ユーザからの世代間配信によってコンテンツを受領したユーザデバイスは、同一セキュアコンテナについてすでに実行された世代間配信の回数が減じられた回数が設定される。

#### 【0192】

「UCS 二次配信可能回数」733は前述の「二次配信」の可能回数を設定したフィールドであり、コンテンツを最初に購入したユーザデバイスは、販売条件（UCP）中の「UCP 二次配信可能回数」に一致する回数が設定され、その後の二次配信に応じて更新、すなわち設定回数がデクリメントされる。

#### 【0193】

このように、コンテンツのユーザ間での配信は、ユーザデバイス内のメモリにコンテンツに応じて格納される使用制御情報（UCS : Usage Control Status）中の「UCS 世代管理情報」、「UCS 二次配信可能回数」に基づいて、それぞれの処理の可否が決定される。「UCS 世代管理情報」はコンテンツの世代間配信毎に更新され、「UCS 二次配信可能回数」はコンテンツの二次配信毎に更新される。

#### 【0194】

図39にコンテンツを格納したセキュアコンテナをサービスプロバイダからユーザデバイスに配信する際の個人識別証明書（IDC）の利用を説明する図を示す。

#### 【0195】

ユーザデバイス810のユーザ820は、まず自己の個人識別証明書（IDC）の発行を個人識別認証局（IDA）830に依頼する。この際、ユーザは、個

人の生体情報、その他の個人情報を提供する。個人識別認証局（IDA）830は、ユーザの正当性を確認した上で、サンプリング情報に基づくテンプレート情報を生成し、テンプレート情報を暗号化して格納した個人識別証明書（IDC）を生成する。

#### 【0196】

生成した個人識別証明書（IDC）は要求に応じて、ユーザデバイス810、あるいはサービスプロバイダ840に配信され、格納される。ユーザ820が例えばサービスプロバイダ840からのコンテンツ配信を受ける際、ユーザの個人認証手続きをサービスプロバイダ840の有する個人識別証明書（IDC）に基づいて実行する。すなわち、ユーザの提供するサンプリング情報と、個人識別証明書（IDC）内のテンプレート情報とを照合して一致した場合は、サンプリング情報を提供したユーザが個人識別証明書（IDC）に対応する正当なユーザであると判定して、コンテンツ配信を実行する。

#### 【0197】

また、ユーザデバイス810の使用の際にも、ユーザデバイス810に格納した個人識別証明書（IDC）に基づいてユーザの個人認証手続きを実行する。すなわち、ユーザの入力するサンプリング情報と、個人識別証明書（IDC）内のテンプレート情報とを照合して一致した場合は、サンプリング情報を提供したユーザが個人識別証明書（IDC）に対応する正当なユーザであると判定して、ユーザデバイスを使用したデータ処理を実行可能とする。

#### 【0198】

このように個人識別証明書（IDC）を使用した個人認証処理は、様々な場所、すなわちユーザデバイスやサービスプロバイダにおいて独自に実行することができる。なお、前述したように、個人識別証明書（IDC）内のテンプレートは、照合処理を実行するシステムの公開鍵で暗号化して格納されている。

#### 【0199】

図40にセキュアコンテナをサービスプロバイダから受領し、ユーザデバイスにおいて個人認証処理を実行して、正当なユーザにのみコンテンツ利用を可能とした処理フローを示す。以下、フローの各ステップについて説明する。

## 【 0 2 0 0 】

ステップ S 7 0 1 では、サービスプロバイダとユーザデバイス間で相互認証を実行し、認証成立を条件（S 7 0 2 で Y e s）として、サービスプロバイダは、セキュアコンテナを抽出し（S 7 0 3）、ユーザデバイスに送信する（S 7 0 4）。なお、相互認証時にセッションキーが生成され、以下のサービスプロバイダとユーザデバイス間でのデータ転送は、必要に応じてセッションキーでの暗号化処理が行なわれる。

## 【 0 2 0 1 】

ユーザデバイスは受信したセキュアコンテナの検証を行なう（S 7 0 5）、検証には、セキュアコンテナ自体の署名検証、コンテナ内の価格情報、販売条件情報（UCP）等の個別データの署名検証処理を含む。

## 【 0 2 0 2 】

コンテナ検証が成功すると（S 7 0 6, Y e s）、ユーザは、サンプリング情報とユーザIDをユーザデバイスに入力（S 7 0 7）し、ユーザデバイスは、セキュアコンテナの価格情報、販売条件情報（UCP）のいずれかから個人識別証明書（IDC）リストを抽出し（S 7 0 8）、ユーザIDに基づいて対応するIDC識別子を検索する（S 7 0 9）。入力ユーザIDに対応するIDC識別子が検出されない場合は、サービスプロバイダの認めたユーザでないと判定され、エラーとなり（S 7 1 0 で N o）、処理は続行されない。

## 【 0 2 0 3 】

個人識別証明書（IDC）リストに入力ユーザIDに対応するIDC識別子が検出された場合（S 7 1 0 で Y e s）は、IDC識別子に基づいて個人識別証明書（IDC）を取得（S 7 1 1）する。個人識別証明書（IDC）は、ユーザデバイスに格納されている場合は、ユーザデバイスに格納されたIDCを用い、ない場合は、個人識別認証局（IDA）、またはサービスプロバイダから取り寄せる。取得した個人識別証明書（IDC）からテンプレートを取り出して、自己の秘密鍵で復号し、テンプレートとサンプリング情報との照合を実行し（S 7 1 2）、照合が成立しない場合（S 7 1 3 で N o）は、エラーとなり、その後の処理が続行されない。具体的にはコンテンツの復号処理が実行されず、コンテンツの

利用が制限される。照合が成立した場合（S713でYes）は、照合成立がサービスプロバイダに通知され、サービスプロバイダはセキュアコンテナに格納された暗号化コンテンツの復号に適用するコンテンツ鍵をユーザデバイスに送信する（S714）。ユーザデバイスでは、サービスプロバイダから受信したコンテンツ鍵を使用して暗号化コンテンツの復号を行ないコンテンツを利用（S715）する。

#### 【0204】

このように、個人識別証明書（IDC）のテンプレートを用いたユーザの個人識別処理を実行し、照合成立により、正当ユーザであることが確認された場合にのみセキュアコンテナに格納されたコンテンツの利用を可能とする構成により、不当なユーザのコンテンツ利用を防止することが可能となる。

#### 【0205】

次に、図41にサービスプロバイダにおいて個人認証処理を実行して、正当なユーザにのみセキュアコンテナを配信する処理フローを示す。以下、フローの各ステップについて説明する。

#### 【0206】

ステップS721では、サービスプロバイダとユーザデバイス間で相互認証を実行する。相互認証時にセッションキーが生成され、以下のサービスプロバイダとユーザデバイス間でのデータ転送は、必要に応じてセッションキーでの暗号化処理が行なわれる。

#### 【0207】

相互認証成立を条件（S722でYes）として、サービスプロバイダは、セキュアコンテナを抽出し（S723）、ユーザデバイスは、サンプリング情報とユーザIDをユーザデバイスに入力（S735）し、これらをサービスプロバイダに送信（S736）する。

#### 【0208】

サービスプロバイダは、セキュアコンテナの価格情報、販売条件情報（UCP）のいずれかから個人識別証明書（IDC）リストを抽出し（S724）、ユーザIDに基づいて対応するIDC識別子を検索する（S725）。入力ユーザI



Dに対応するIDC識別子が検出されない場合は、サービスプロバイダの認めたユーザでないこととなり、エラーとなり（S726でNo）、処理は続行されない。

#### 【0209】

個人識別証明書（IDC）リストに入力ユーザIDに対応するIDC識別子が検出された場合（S726でYes）は、IDC識別子に基づいて個人識別証明書（IDC）を取得（S727）する。個人識別証明書（IDC）は、サービスプロバイダに格納されている場合は、サービスプロバイダに格納されたIDCを用い、ない場合は、個人識別認証局（IDA）から取り寄せる。取得した個人識別証明書（IDC）からテンプレートを取り出して、自己の秘密鍵で復号し、テンプレートとサンプリング情報との照合を実行し（S728）、照合が成立しない場合（S729でNo）は、エラーとなり、その後の処理が続行されない。具体的にはセキュアコンテナの配信が実行されない。照合が成立した場合（S729でYes）は、正当なユーザであると判定され、その後の処理が続行される。具体的にはサービスプロバイダからユーザデバイスに対するセキュアコンテナ、およびコンテンツ鍵の配信が実行される（S730）。

#### 【0210】

サービスプロバイダは、セキュアコンテナをユーザデバイスに送信し、ユーザデバイスは受信したセキュアコンテナの検証を行なう（S731）、検証には、セキュアコンテナ自体の署名検証、コンテナ内の価格情報、販売条件情報（UCP）等の個別データの署名検証処理を含む。コンテナ検証が成功すると（S732, Yes）、ユーザデバイスにおいてセキュアコンテナのコンテンツ利用が可能となる。

#### 【0211】

このように、サービスプロバイダ側で、個人識別証明書（IDC）のテンプレートを用いたユーザの個人識別処理を実行し、照合成立により、正当ユーザであることが確認された場合にのみセキュアコンテナの配信を実行する構成により、不当なユーザに対するコンテンツ配信を防止することが可能となる。

#### 【0212】

次に、ユーザデバイス間におけるセキュアコンテナの配信処理における個人識別証明書（IDC）の利用形態について説明する。

#### 【0213】

図42にセキュアコンテナを利用したコンテンツのユーザ間の配信処理形態を示す。サービスプロバイダ（SP）は、コンテンツの利用に対する価格情報を生成して、価格情報、販売条件（UCP）の少なくともいずれか、あるいは両者にコンテンツ利用の許可されたユーザの個人識別証明書（IDC）のリストを格納し、電子署名を行なってセキュアコンテナを形成し、ユーザデバイス1, 920に送付する。

#### 【0214】

ユーザデバイス1, 920の利用を行なうユーザ940, 945は、正当なコンテンツの利用が認められたユーザである場合、コンテンツに対応するセキュアコンテナの価格情報、販売条件（UCP）、またはセキュアコンテナのユーザデバイス格納処理の際にユーザデバイスにおいて生成され格納される使用制御情報（UCS）のいずれかに格納された個人識別証明書（IDC）のリストにユーザのIDC識別子が格納されることになる。ユーザデバイス1, 920の格納コンテンツを利用する場合、セキュアコンテナのIDCリストに基づく個人認証処理を実行する。コンテンツ利用を要求するユーザにサンプリング情報の入力を求め、入力されたサンプリング情報と格納された個人識別証明書（IDC）内のテンプレートとの照合を実行し、照合が成立した場合にのみ、コンテンツ利用を許可する。

#### 【0215】

さらに、セキュアコンテナは、前述の通り、ユーザデバイス間での配信が可能である。セキュアコンテナがユーザデバイス1, 920から、ユーザデバイス2, 930に移動された場合、ユーザ940, 945は、ユーザデバイス2, 930においてコンテンツの利用を行なう場合においても、セキュアコンテナの価格情報、販売条件（UCP）、または使用制御情報（UCS）のIDCリストに基づく個人認証処理を実行する。コンテンツ利用を要求するユーザにサンプリング情報の入力を求め、入力されたサンプリング情報と格納された個人識別証明書（

IDC) 内のテンプレートとの照合を実行し、照合が成立を条件としてコンテンツ利用を許可する。

【0216】

このように、セキュアコンテナの移動があった場合においても、セキュアコンテナに当初格納された価格情報、販売条件 (UCP) の個人識別証明書 (IDC) リストは不変であり、またセキュアコンテナの販売条件 (UCP) に基づいて生成される使用制御情報 (UCS) の IDC リストも不変であり、これらの IDC リストに基づいてコンテンツの利用者が正当なユーザにのみ制限することが可能となる。

【0217】

次に、図 4 3 にセキュアコンテナを利用したコンテンツのユーザ間の配信処理、ユーザの個人認証の異なる形態を示す。図 4 3 に示す処理は、ユーザデバイスの使用制限、すなわちアクセス制限をユーザデバイスに格納した個人識別証明書 (IDC) に基づく個人認証処理により実行し、さらに、コンテンツの使用に際して、セキュアコンテナの価格情報、販売条件 (UCP)、または使用制御情報 (UCS) の IDC リストに基づく個人認証処理を実行する 2 つの認証を実行する形態である。

【0218】

ユーザデバイス 1, 950 を使用するユーザ A, ユーザ B は、個人識別認証局 (IDA) 970 に予めサンプリング情報を提示して、サンプリング情報に基づくテンプレート情報を格納した個人識別証明書 (IDC) の発行依頼を行なう。発行された個人識別証明書 (IDC) は、使用するユーザデバイス 1, 950 に格納する。

【0219】

ユーザデバイス 950 は使用開始にあたり、デバイスに格納された個人識別証明書 (IDC) 955 に基づく個人認証処理を実行し、使用を要求するユーザにサンプリング情報の入力を求め、入力されたサンプリング情報と格納された個人識別証明書 (IDC) 内のテンプレートとの照合を実行し、照合が成立した場合にのみ、ユーザデバイス 1, 950 の使用を許可する。

## 【 0 2 2 0 】

さらに、セキュアコンテナ 9 9 0 のコンテンツの利用を行なう際には、セキュアコンテナの価格情報、販売条件（UCP）、または使用制御情報（UCS）の IDC リストに基づく個人認証処理を実行する。ここでユーザに対応する IDC リストが検出されないか、または検出されても入力サンプリング情報と照合が成立しない場合はコンテンツの利用が許可されない。

## 【 0 2 2 1 】

すなわち、セキュアコンテナ 9 9 0 の格納コンテンツをユーザデバイス 1, 9 5 0 において利用する際は、ユーザデバイスに格納された個人識別証明書（IDC）に基づく個人認証が成立し、さらに、セキュアコンテナの価格情報、販売条件（UCP）、または使用制御情報（UCS）の IDC リストに基づく個人認証処理が成立することが要件となる。

## 【 0 2 2 2 】

セキュアコンテナは、デバイス間で移動することが可能であり、ユーザデバイス 2, 9 6 0 に移動した場合は、同様にユーザデバイス 2, 9 6 0 に格納された個人識別証明書（IDC）に基づく個人認証、さらに、セキュアコンテナの価格情報、販売条件（UCP）、または使用制御情報（UCS）の IDC リストに基づく個人認証処理が実行される。

## 【 0 2 2 3 】

図 4 3 の構成では、ユーザデバイス 1, 9 5 0 にはユーザ A, B の個人識別証明書（IDC）9 5 5 が格納されており、セキュアコンテナにはユーザ A, B, C のリスト 9 9 2 が格納されているので、ユーザ A, B のみがユーザデバイス 1, 9 5 0 を使用してコンテンツの利用が可能となり、ユーザデバイス 2, 9 6 0 にはユーザ A, C の個人識別証明書（IDC）9 6 5 が格納されており、セキュアコンテナにはユーザ A, B, C のリスト 9 9 2 が格納されているので、ユーザ A, C のみがユーザデバイス 2, 9 6 0 を使用してコンテンツの利用が可能となる。

## 【 0 2 2 4 】

なお、図 4 3 の構成例は、各ユーザデバイスにおいては格納 IDC のみとの照

合処理を実行することを条件とした認証処理を行なうように設定したシステムである。個人識別証明書（IDC）を個人識別認証局（IDA）に登録済みのすべてのユーザが使用可能なデバイスとして設定する場合は、デバイスのアクセス権制御をデバイスに格納したIDCのみならず、IDAに接続してIDAに格納した個人識別証明書（IDC）の格納テンプレートと入力サンプリング情報との比較を実行して認証処理を行なうようにしてもよい。

#### 【0225】

なお、ユーザデバイス間におけるセキュアコンテナの配信、利用処理においてセキュアコンテナのIDCリストに基づく個人識別証明書（IDC）を利用した個人認証を実行してコンテンツの利用制限を実行する処理例を図44、45の処理フローに従って説明する。このフローにおいては、ユーザデバイスのアクセス制限については含まない処理として説明する。

#### 【0226】

図44にセキュアコンテナをユーザデバイスAから受領し、ユーザデバイスBにおいて個人認証処理を実行して、正当なユーザにのみコンテンツ利用を可能とした処理フローを示す。以下、フローの各ステップについて説明する。

#### 【0227】

ステップS751では、ユーザデバイスAとユーザデバイスB間で相互認証を実行し、認証成立を条件（S752でYes）として、ユーザデバイスAは、セキュアコンテナを抽出し（S753）、ユーザデバイスBに送信する（S754）。なお、相互認証時にセッションキーが生成され、以下のユーザデバイス間でのデータ転送は、必要に応じてセッションキーでの暗号化処理が行なわれる。

#### 【0228】

ユーザデバイスBは受信したセキュアコンテナの検証を行なう（S755）、検証には、セキュアコンテナ自体の署名検証、コンテナ内の価格情報、販売条件情報（UCP）等の個別データの署名検証処理を含む。

#### 【0229】

コンテナ検証が成功すると（S756, Yes）、コンテンツ利用を要求するユーザは、サンプリング情報とユーザIDをユーザデバイスBに入力（S757

）し、ユーザデバイスBは、使用制御情報（UCS）から個人識別証明書（IDC）リストを抽出し（S758）、ユーザIDに基づいて対応するIDC識別子を検索する（S759）。入力ユーザIDに対応するIDC識別子が検出されない場合は、サービスプロバイダの認めたユーザでないこととなり、エラーとなり（S760でNo）、処理は続行されない。

#### 【0230】

個人識別証明書（IDC）リストに入力ユーザIDに対応するIDC識別子が検出された場合（S760でYes）は、IDC識別子に基づいて個人識別証明書（IDC）を取得（S761）する。個人識別証明書（IDC）は、ユーザデバイスBに格納されている場合は、ユーザデバイスBに格納されたIDCを用い、ない場合は、個人識別認証局（IDA）、またはサービスプロバイダから取り寄せる。取得した個人識別証明書（IDC）からテンプレートを取り出して、自己の秘密鍵で復号し、テンプレートとサンプリング情報との照合を実行し（S762）、照合が成立しない場合（S763でNo）は、エラーとなり、その後の処理が続行されない。具体的にはコンテンツの復号処理が実行されず、コンテンツの利用が制限される。照合が成立した場合（S763でYes）は、照合成立がユーザデバイスAに通知され、ユーザデバイスAはセキュアコンテナに格納された暗号化コンテンツの復号に適用するコンテンツ鍵をユーザデバイスBに送信する（S764）。ユーザデバイスBでは、ユーザデバイスAから受信したコンテンツ鍵を使用して暗号化コンテンツの復号を行ないコンテンツを利用（S765）する。

#### 【0231】

このように、個人識別証明書（IDC）のテンプレートを用いたユーザの個人識別処理を実行し、照合成立により、正当ユーザであることが確認された場合にのみセキュアコンテナに格納されたコンテンツの利用を可能とする構成により、セキュアコンテナがユーザデバイス間で配信された後も、不当なユーザのコンテンツ利用を防止することが可能となる。

#### 【0232】

次に、図45にコンテンツを配信する前に配信元において個人認証処理を実行

して、正当なユーザにのみセキュアコンテナを配信する処理フローを示す。以下、フローの各ステップについて説明する。

#### 【0233】

ステップS771では、ユーザデバイスAとユーザデバイスB間で相互認証を実行する。相互認証時にセッションキーが生成され、以下のサービスプロバイダとユーザデバイス間でのデータ転送は、必要に応じてセッションキーでの暗号化処理が行なわれる。

#### 【0234】

相互認証成立を条件（S772でYes）として、ユーザデバイスAは、セキュアコンテナを抽出し（S773）、ユーザデバイスBは、サンプリング情報とユーザIDをユーザデバイスに入力（S785）し、これらをユーザデバイスAに送信（S786）する。

#### 【0235】

ユーザデバイスA、セキュアコンテナの価格情報、販売条件情報（UCP）、または使用制御情報（UCS）のいずれかから個人識別証明書（IDC）リストを抽出し（S774）、ユーザIDに基づいて対応するIDC識別子を検索する（S775）。入力ユーザIDに対応するIDC識別子が検出されない場合は、サービスプロバイダの認めたユーザでないと判定され、エラーとなり（S776でNo）、処理は続行されない。

#### 【0236】

個人識別証明書（IDC）リストに入力ユーザIDに対応するIDC識別子が検出された場合（S776でYes）は、IDC識別子に基づいて個人識別証明書（IDC）を取得（S777）する。個人識別証明書（IDC）は、サービスプロバイダに格納されている場合は、サービスプロバイダに格納されたIDCを用い、ない場合は、個人識別認証局（IDA）から取り寄せる。取得した個人識別証明書（IDC）からテンプレートを取り出して、自己の秘密鍵で復号し、テンプレートとサンプリング情報との照合を実行し（S778）、照合が成立しない場合（S779でNo）は、エラーとなり、その後の処理が続行されない。具体的にはセキュアコンテナおよびコンテンツ鍵の配信が実行されない。照合が成

立した場合（S 7 7 9 で Y e s ）は、正当なユーザであると判定され、その後の処理が続行される。具体的にはセキュアコンテナおよびコンテンツ鍵のユーザデバイス B に対する配信が実行される。

#### 【 0 2 3 7 】

ユーザデバイス A がセキュアコンテナをユーザデバイス B に送信すると、ユーザデバイス B は受信したセキュアコンテナの検証を行なう（S 7 8 1）、検証には、セキュアコンテナ自体の署名検証、コンテナ内の価格情報、販売条件情報（UCP）等の個別データの署名検証処理を含む。コンテナ検証が成功すると（S 7 8 2, Y e s）、ユーザデバイス B においてセキュアコンテナのコンテンツ利用が可能となる。

#### 【 0 2 3 8 】

このように、ユーザデバイス A 側で、個人識別証明書（IDC）のテンプレートを用いたユーザの個人識別処理を実行し、照合成立により、正当ユーザであることが確認された場合にのみセキュアコンテナの配信を実行する構成により、不当なユーザに対するコンテンツ配信を防止することが可能となる。

#### 【 0 2 3 9 】

次に、図 4 6 にユーザデバイス間でのセキュアコンテナの転送処理を実行するユーザデバイス構成を中心としたブロック図を示す。図 4 6 を用いてセキュアコンテナの転送、コンテンツ使用制御情報（UCS）生成、格納処理について説明する。

#### 【 0 2 4 0 】

図 4 6 のサービスプロバイダ 1 8 1 0 が、セキュアコンテナの最初の流通（一次配布）を行なう。サービスプロバイダ 1 8 1 0 は、コンテンツデータベース 1 8 1 2 にコンテンツを格納し、さらに、ユーザ情報データベース 1 8 1 3 にユーザ情報を格納している。サービスプロバイダ 1 8 1 0 は、制御部 1 8 1 1 の制御のもとに暗号処理部 1 8 1 4 において、セキュアコンテナの転送処理に必要な転送先との相互認証処理、転送データに対する署名処理等を実行する。暗号処理部 1 8 1 4 は、これら各暗号処理に必要となる鍵情報、さらに、先に説明した公開鍵証明書発行局（CA）の公開鍵、公開鍵証明書発行局（CA）の発行した公開



鍵証明書等を保持したメモリを有している。また、データベース1813にはサービス提供ユーザに関する個人識別証明書（IDC）を格納している。必要に応じてIDCを使用して個人識別装置1816においてサンプリング情報との照合処理による個人認証を実行する。

#### 【0241】

サービスプロバイダ1810は、ユーザデバイスA1820に対してセキュアコンテナを通信部1815を介して転送する。セキュアコンテナは先に説明したように、販売条件（UCP）、価格情報を含み、少なくともいずれかに個人識別証明書（IDC）リストを含む。

#### 【0242】

また、図46に示すクリアリングセンタ1840がコンテンツ流通に伴うコンテンツ利用料の決済（電子マネー上のデータなど）処理を行なう。クリアリングセンタ1840は、通信部1845を介して行われる決済用の受領ログ受信または発行ログ送信において各デバイスと認証処理を実行し、また送受信データに対する署名処理、署名検証処理を実行するための暗号処理部1844を有し、また、ユーザ管理、ユーザ残高管理用の各種のデータを格納したデータベース1842を有する。暗号処理部1844には、各暗号処理に必要な鍵情報、公開鍵証明書発行局（CA）の公開鍵、公開鍵証明書発行局（CA）の発行した公開鍵証明書等を保持したメモリを有している。制御部1841は、データ送受信、暗号処理部における暗号処理時のデータ転送等の制御を行なう。また、データベース1842にはサービス提供ユーザに関する個人識別証明書（IDC）を格納している。必要に応じてIDCを使用して個人識別装置1846においてサンプリング情報との照合処理による個人認証を実行する。

#### 【0243】

サービスプロバイダ1810は、ユーザデバイスA1820に対してセキュアコンテナを通信部1815を介して転送して、ユーザデバイスA1820が通信部1827を介してこれを受信し、購入処理を実行する。購入処理においては、記憶部1825に格納した個人識別証明書（IDC）による個人認証を実行する。なお、個人識別証明書（IDC）がない場合は、サービスプロバイダ1810

において個人認証処理を実行してもよい。ユーザデバイス A 1 8 2 0 は、制御部 1 8 2 1 の制御のもとに暗号処理部 1 8 2 2 においてセキュアコンテナの販売条件 (UCP) 等に基づいてコンテンツ使用制限情報 (UCS) を生成して、これをフラッシュメモリ等のメモリ 1 8 2 4 に格納する。コンテンツ使用制限情報 (UCS) には前述したように販売条件 (UCP) に格納した個人識別証明書 (IDC) リストを承継したリストを含む。

#### 【 0 2 4 4 】

ユーザデバイス A 1 8 2 0 は、例えば電子マネー 1 8 2 8 によるコンテンツ利用料金支払処理を行なう。利用ログを暗号処理部 1 8 2 2 において生成して、通信部 1 8 2 7 を介してサービスプロバイダ 1 8 1 0 に送信する。ユーザデバイス A 1 8 2 0 が受信したセキュアコンテナは、ハードディスク等の記憶部 1 8 2 5 に格納される。サービスプロバイダ 1 8 1 0 は、ユーザデバイス A 1 8 2 0 から送信された利用ログの検証をして、検証が済むと、コンテンツ鍵をセッション鍵で暗号化してユーザデバイス A 1 8 2 0 に送信する。ユーザデバイス A 1 8 2 0 は、暗号化されたコンテンツ鍵をセッション鍵で復号し、これをさらにユーザデバイス A 1 8 2 0 固有の保存鍵で暗号化してメモリ 1 8 2 4 に格納する。

#### 【 0 2 4 5 】

ユーザデバイス A 1 8 2 0 は、データ再生部 1 8 2 6 でのコンテンツ再生等、コンテンツ利用に際しては、メモリ 1 8 2 4 に保存したコンテンツ鍵を保存鍵で復号して、復号したコンテンツ鍵を用いて記憶部 1 8 2 5 に格納されたセキュアコンテナ中のコンテンツを復号処理してデータ再生部 1 8 2 6 において再生する。なお、セキュアコンテナ中のコンテンツの復号処理に際しては、その前ステップとして、メモリ 1 8 2 4 に格納されたコンテンツ使用制限情報 (UCS) の再生残り回数等の設定条件を判定し、条件がクリアされた場合には復号が可能となる。

#### 【 0 2 4 6 】

さらに、セキュアコンテナをユーザデバイス A 1 8 2 0 からユーザデバイス B 1 8 3 0 に配信する場合は、ユーザデバイス A 1 8 2 0 は、メモリ 1 8 2 4 からコンテンツ使用制限情報 (UCS) を読み出し、暗号処理部 1 8 2 2 内で保存鍵

で復号化（暗号化されていない場合は復号処理は不要）し、UCSの「UCS世代管理情報」、「UCS二次配信可能回数」を判定し、新たな配信が可能と判定された場合には、ユーザデバイスB1830に対してセキュアコンテナを通信部1827を介して転送して、ユーザデバイスB1830が通信部1837を介してこれを受信し、購入処理を実行する。

## 【0247】

なお、セキュアコンテナの配信時には前述の個人認証処理が実行される。個人認証処理は、前述の図45のフローを用いて説明したようにセキュアコンテナの配信元のユーザデバイスAの個人識別装置1829で実行するか、あるいは図44のフローを用いて説明したように配信先のユーザデバイスBの個人識別装置1839のいずれかで実行する。また、その他のサービプロバイダ、あるいは個人識別認証局（IDA）において実行するようにしてもよい。

## 【0248】

個人認証が成立すると、ユーザデバイスB1830は、制御部1831の制御のもとに暗号処理部1832においてセキュアコンテナの販売条件（UCP）とユーザデバイスA1820のUCS情報等に基づいて、新たな「UCS世代管理情報」、「UCS二次配信可能回数」を設定したコンテンツ使用制限情報（UCS-B）を生成して、これをフラッシュメモリ等のメモリ1834に格納する。

## 【0249】

この際に生成するUCS-Bは、ユーザデバイスA1820のコンテンツ利用履歴を継承したものとなる。UCS-Bの「UCS世代管理情報」はUCS-Aの「UCS世代管理情報」より1つ減じた回数として設定される。UCS-Bの「UCS二次配信可能回数」はUCS-Aの「UCS二次配信可能回数」より1つ減じた回数として設定する構成と、セキュアコンテナ内の「UCP二次配信可能回数」と同一回数を新たに設定する構成とがある。

## 【0250】

ユーザデバイスB1830は、電子マネー1838によるコンテンツ利用料金支払処理、すなわち利用ログを暗号処理部1832において生成して、通信部1837を介してユーザデバイスA1820に送信する。ユーザデバイスB183

0 が受信したセキュアコンテナは、ハードディスク等の記憶部 1 8 3 5 に格納される。ユーザデバイス A 1 8 2 0 は、ユーザデバイス B 1 8 3 0 から送信された利用ログの検証をして、検証が済むと、メモリ 1 8 2 4 からコンテンツ鍵を読み出し、これを保存鍵で復号した後、コンテンツ鍵をセッション鍵で暗号化してユーザデバイス B 1 8 3 0 に送信する。ユーザデバイス B 1 8 3 0 は、暗号化されたコンテンツ鍵をセッション鍵で復号し、これをさらにユーザデバイス B 1 8 3 0 固有の保存鍵で暗号化してメモリ 1 8 3 4 に格納する。

## 【 0 2 5 1 】

また、不正な改竄により設定を超えた使用を行なうと、同一セキュアコンテナに基づいて生成された受領ログ数が、セキュアコンテナ中の販売条件（UCP）に含まれる「UCP 世代管理情報」の設定を超えることとなるため、クリアリングセンタ 1 8 4 0 に送付された場合に無効と判定される。受領ログには、コンテンツ ID 等の情報とともに、セキュアコンテナに記録された「UCP 世代管理情報」が記録されており、クリアリングセンタ 1 8 4 0 における決済処理においては、「UCP 世代管理情報」の設定を超える受領ログを受信した場合はこれを無効とする。なお、ユーザ間配信の認められない設定のなされたコンテンツに基づいて生成された受領ログについても、その受領ログを無効とする処理を実行する。

## 【 0 2 5 2 】

ユーザデバイス B 1 8 3 0 は、データ再生部 1 8 3 6 でのコンテンツ再生等、コンテンツ利用に際しては、メモリ 1 8 3 4 に保存したコンテンツ鍵を保存鍵で復号して、復号したコンテンツ鍵を用いて記憶部 1 8 3 5 に格納されたセキュアコンテナ中のコンテンツを復号処理してデータ再生部 1 8 3 6 において再生する。なお、セキュアコンテナ中のコンテンツの復号処理に際しては、メモリ 1 8 3 4 に格納されたコンテンツ使用制限情報（UCS）に設定された再生残り回数等の利用可能状況が判定され、設定条件範囲内でコンテンツの利用、すなわち復号が可能となる。

## 【 0 2 5 3 】

セキュアコンテナを用いたコンテンツ配信では、サービスプロバイダとユーザ

デバイス間の一次配布、さらに複数のユーザデバイス間での二次配布（世代間配信または二次配信）において、個人識別証明書（IDC）によるユーザ確認が可能となり、また、コンテンツ利用は、セキュアコンテナ中の販売条件（UCP）に含まれる「UCP世代管理情報」、「UCP二次配信可能回数」によって制限された範囲に制限される。また一次配布、二次配布（世代間配信または二次配信）に伴うコンテンツ利用料金回収もセキュアコンテナ中の価格情報、販売条件等に基づいて生成される受領ログに従って自動的に処理可能となるため、決済処理のための新たな処理が不要となる。

## 【 0 2 5 4 】

## 〔 7. 個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンク 〕

次に、個人識別証明書（IDC）と公開鍵証明書（PKC）とを関連付ける構成、すなわちリンク構成について説明する。

## 【 0 2 5 5 】

個人識別証明書（IDC）と公開鍵証明書（PKC）とは関連付けて管理することが、様々な場面において有効となる。例えば、個人識別証明書（IDC）と、該個人識別証明書の格納テンプレートの暗号化に適用した公開鍵の公開鍵証明書とを関連付けるリンクを構成したり、特定のサービスプロバイダ等、データ通信先との接続処理の際の、個人認証、相互認証または暗号処理データ通信を実行する際に適用する個人識別証明書と公開鍵証明書との組み合わせについてのリンクを構成することで、一方の証明書に基づいて他方の証明書を特定することが可能となる。

## 【 0 2 5 6 】

個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンクは1対1のリンク、すなわち1つの個人識別証明書（IDC）と、1つの公開鍵証明書（PKC）とをリンクさせる態様の他に、1対多、多対1、多対多のリンク態様がある。PKCとIDCの対応が1対1とは、個人識別証明書（IDC）によって識別される唯一の個人に唯一の公開鍵証明書（PKC）が対応する場合で、例えば使用デバイスと、そのデバイスを使用する個人が1対1に対応する場合である。

## 【 0 2 5 7 】

PKCとIDCの対応が1対N（Nは2以上）とは、複数の個人識別証明書（IDC）によって識別される複数の個人と公開鍵証明書が非対応。すなわち、デバイスを複数人で共有する場合等である。PKCとIDCの対応がM対1（Mは2以上）とは、個人識別証明書（IDC）によって識別される唯一の個人が使用する、または使用できる公開鍵証明書が複数ある場合である。PKCとIDCの対応がM対N（M，Nは2以上）とは、複数の個人識別証明書（IDC）によって識別される複数の個人が使用する、または使用できる公開鍵証明書が複数あり、かつ、デバイスを共有している場合である。

## 【0258】

また、個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンク態様には、リンク方向、すなわちいずれか一方の証明書から他方の証明書を導くことのみが可能な一方向リンク（または片方向リンク、有方向リンク）と、いずれの証明書からでも他方の証明書を導くことが可能な双方向リンクとがある。

## 【0259】

図47，48に1対1、1対多、多対1、多対多の個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンク態様のそれぞれについて示す。いずれの場合も個人識別証明書（IDC）は、個人識別認証局（IDA）によって発行され個人識別認証局（IDA）の署名が付加された証明書であり、公開鍵証明書（PKC）は認証局（CA）によって発行され、認証局（CA）の署名が付加されている。

## 【0260】

リンクの実現方法としては、いずれの場合においても、以下に示す各種の実現方法がある。

① PKC識別番号をIDCに埋め込む。

（IDCからPKCへの1方向リンク）

② IDC識別番号をPKCに埋め込む。

（PKCからIDCへの1方向リンク）

③ リンク構造体IDをIDC、PKCに埋め込む。リンク構造体はリンク構造体IDによって識別され、リンク関係のIDC識別番号、PKC識別番号を持つ。

( I D C、 P K C の双方向リンク)

- ④ P K C 識別番号と I D C 識別番号の組を証明書外に記録する。

( I D C から P K C への 1 方向リンク)

- ⑤ P K C 識別番号と I D C 識別番号の組を証明書外に記録する。

( P K C から I D C への 1 方向リンク)

- ⑥ P K C 識別番号と I D C 識別番号の組を証明書外に記録する。

( I D C、 P K C の双方向リンク)

- ⑦ I D C 内に P K C を格納する。

( I D C から P K C への 1 方向リンク)

- ⑧ P K C 内に I D C を格納する。

( P K C から I D C への 1 方向リンク)

- ⑨ 各証明書内にリンク情報問い合わせ番号、問い合わせ情報を格納する。

( P K C、 I D C のいずれか 1 方向、または双方向リンク)

【 0 2 6 1 】

上述のように、リンク情報の格納態様としては、①、②に示すように、個人識別証明書 ( I D C ) または公開鍵証明書 ( P K C ) 自身の内部に、リンク証明書の識別番号を格納 ( 埋め込む ) する方法、③に示すように、リンク関係にある各証明書の識別番号の対応を示すリンク構造体を生成してそのリンク構造体の識別子 ( I D ) を関連付けた個人識別証明書 ( I D C ) または公開鍵証明書 ( P K C ) に記録する方法、すなわち、リンク識別データとしてのリンク構造体識別子と、リンクを構成する公開鍵証明書識別子と、個人識別証明書識別子とをデータとして格納する構成、さらに、④、⑤、⑥に示すように、それぞれの証明書とは、異なる外部、例えばネットワーク上に配置したリンク情報管理センター等の機関において、個人識別証明書 ( I D C ) と公開鍵証明書 ( P K C ) とのリンク情報を集積して管理し、必要に応じてリンク情報を抽出可能にする構成等がある。各リンク態様の具体的構成について、説明する。

【 0 2 6 2 】

( I D C 内に P K C を格納)

前述したように個人識別のためのテンプレート情報の個人識別証明書 ( I D C

）における格納態様の一態様には、公開鍵でテンプレートを暗号化して格納する構成がある。このテンプレートを暗号化した公開鍵に対応して生成された公開鍵証明書（PKC）が、個人識別証明書（IDC）のリンク公開鍵証明書（PKC）として設定され、このリンク公開鍵証明書（PKC）を個人識別証明書（IDC）に格納する。図49（a）にリンク公開鍵証明書（PKC）の個人識別証明書（IDC）に対する格納態様を説明する図を示す。

## 【0263】

図49（a）に示すように、個人識別証明書（IDC）には、暗号化されたテンプレート、およびそのテンプレート暗号化に適用した公開鍵に対応する公開鍵証明書（PKC）が格納される。なお、テンプレート暗号化に適用する公開鍵は、前述のように、ユーザまたはユーザデバイスの公開鍵、サービスプロバイダ（SP）の公開鍵、または、個人識別認証局（IDA）の公開鍵のいずれかであり、格納される公開鍵証明書（PKC）は、そのテンプレート暗号化に適用した公開鍵の公開鍵証明書（PKC）である。このようなリンク構成を採用することにより、個人識別証明書（IDC）と、テンプレート（Template）を暗号化した公開鍵の公開鍵証明書（PKC）が強く結びつき、2種類の証明書が不可分になる。ただし、このリンク構成を採用する場合は、IDC有効期限年月日 $\leq$ PKC有効期限年月日として設定する。すなわち、IDCに格納されるPKCはIDCの有効期限において常に有効である設定とすることが好ましい。

## 【0264】

（PKC内にIDCを格納）

また、テンプレートを暗号化した公開鍵に対応して生成された公開鍵証明書（PKC）の内部に、公開鍵証明書（PKC）のリンク個人識別証明書（IDC）を格納した構成例を図49（b）に示す。

## 【0265】

図49（b）に示すように、公開鍵証明書（PKC）には、その公開鍵証明書（PKC）に対応する公開鍵を適用して暗号化されたテンプレート情報を持つ個人識別証明書（IDC）が格納される。なお、テンプレート暗号化に適用する公開鍵は、前述のように、ユーザまたはユーザデバイスの公開鍵、サービスプロバ



イダ（SP）の公開鍵、または、個人識別認証局（IDA）の公開鍵のいずれかであり、個人識別証明書（IDC）を格納した公開鍵証明書（PKC）は、そのテンプレート暗号化に適用した公開鍵の公開鍵証明書（PKC）である。このようなリンク構成を採用することにより、個人識別証明書（IDC）と、テンプレート（Template）を暗号化した公開鍵の公開鍵証明書（PKC）が強く結びつき、2種類の証明書が不可分になる。なお、個人識別証明書（IDC）自体は独立に存在する。また、このリンク構成を採用する場合は、PKC有効期限年月日＜＝IDC有効期限年月日として設定する。すなわち、PKCに格納されるIDCはPKCの有効期限において常に有効である設定とすることが好ましい。

#### 【0266】

（リンク証明書の識別子を証明書に格納）

次にリンクする証明書の識別子、例えば各証明書に対応して設定された固有の識別番号を被リンク証明書内のデータとして格納する態様について説明する。

#### 【0267】

図50（a）に公開鍵証明書（PKC）の識別番号を個人識別証明書（IDC）に格納する構成例、図50（b）に個人識別証明書（IDC）の識別番号を公開鍵証明書（PKC）に格納する構成例を示す。

#### 【0268】

図50（a）に示す公開鍵証明書（PKC）の識別番号を個人識別証明書（IDC）に格納する場合の公開鍵証明書（PKC）は、前述の例と同様、個人識別証明書（IDC）に格納されたテンプレートの暗号化に適用した公開鍵に対応する公開鍵証明書（PKC）である。この場合、個人識別証明書（IDC）の発行以前に公開鍵証明書（PKC）が発行済みであることが条件となる。また、有効期限の切れた公開鍵証明書（PKC）のリンク情報を格納しても無意味であるので、IDC有効期限年月日＜＝PKC有効期限年月日として設定された関係であることが好ましい。この構成は、PKCをIDC内部に格納する必要がない場合、PKCをIDCに伴って配布することが好ましくない場合等に利用される。

#### 【0269】

また、図50（b）に示す個人識別証明書（IDC）の識別番号を公開鍵証明

書（PKC）に格納する場合は、個人識別証明書（IDC）に格納されたテンプレートの暗号化に適用した公開鍵に対応する公開鍵証明書（PKC）のみならず、個人識別証明書（IDC）に何らかの関連を持つ公開鍵証明書（PKC）の識別子を格納することが可能である。1つの個人識別証明書（IDC）に複数の個人識別証明書（IDC）を関係づけることが可能である。IDCの有効期限年月日とPKCの有効期限年月日の大小関係は、それぞれの証明書の有効性に影響を受けない。ただし、IDCのテンプレートを暗号化するために使用した公開鍵の証明書だけは、その有効期限が $IDC \leq PKC$ でなくてはならない。

#### 【0270】

この構成の使用例としては、個人識別証明書（IDC）を使って機器のアクセスに対して個人認証を行った後、サービス毎に公開鍵ペアが必要となる場合、複数のリンク公開鍵証明書（PKC）を利用する場合がある。

#### 【0271】

（PKC，IDCの組情報を別管理）

次に、個人識別証明書（IDC）と公開鍵証明書（PKC）との組情報（リンク情報）をIDC，PKCとは別のリンク管理用データとして保持し、IDC，PKC内には、リンク管理用データにアクセス可能な情報を格納した形態について説明する。

#### 【0272】

図51、図52にリンク管理用データを用いた管理構成例を示す。図51（a）は、個人識別証明書（IDC）と公開鍵証明書（PKC）との識別子（番号）と、それぞれの有効期限を格納した組情報（リンク情報）を関係データとして保持した構成である。本構成の特徴は、各証明書の登録・発行タイミングを独立とすることができること。証明書関係の記録を必要な場所で生成し管理することで他に影響を与えることがないことがある。関係データの有効期限は、リンク関係のある各証明書の有効期限内、最も短い期限内に設定することが好ましい。一つのIDCで複数のサービスにおける個人認証を行う場合で、各サービス毎に異なる公開鍵ペアを使用する必要がある場合等のリンク管理に有効な形態である。

#### 【0273】

図 5 1 ( b ) は、個人識別証明書 ( I D C ) と公開鍵証明書 ( P K C ) との識別子 ( 番号 ) と、それぞれの有効期限を格納した組情報 ( リンク情報 ) を関係データとして保持するとともに、組情報を識別するための識別子としての組情報シリアル番号を各証明書に格納した構成である。組情報のシリアル番号は、組情報の管理主体が割り当てる組情報固有の識別データである。リンク関係を持つ P K C , I D C の発行に際しては、組情報のシリアル番号データを内部データとして格納する。本構成の特徴は、組情報データの関連情報の追加・変更・削除操作が可能であり、これらの操作が証明書自体に影響を与えないことである。本構成は、例えば、サービスプロバイダにおいて I D C と P K C 、およびサービス関連情報を管理する要請の下、サービス提供対象の I D C 、 P K C 情報を組情報を用いて管理する形態において有効な構成である。

## 【 0 2 7 4 】

図 5 2 ( c ) は、個人識別証明書 ( I D C ) と公開鍵証明書 ( P K C ) に、組情報を識別するための識別子としての組情報シリアル番号を格納し、この組情報を一次情報として定義し、さらに、関連情報を二次情報として、一次情報からアクセス可能な構成としたものである。必要に応じて二次情報から一次情報に対するアクセスも可能な構成とする。一次情報に関連する二次情報は、複数、分散して管理することが可能であり、シリアル番号は P K C 、 I D C の必要な証明書に保存するよう登録発行依頼を行う。関連情報の追加・変更・削除操作は証明書自体に影響を与えない。

## 【 0 2 7 5 】

図 5 2 ( d ) は、個人識別証明書 ( I D C ) と公開鍵証明書 ( P K C ) との識別子 ( 番号 ) を格納した組情報 ( リンク情報 ) を関係データとして保持するとともに、この組情報を一次情報として定義し、さらに、関連情報を二次情報として、一次情報からアクセス可能な構成としたものである。必要に応じて二次情報から一次情報に対するアクセスも可能な構成とする。

## 【 0 2 7 6 】

関連情報を複数の場所に分散して管理する場合は、一次情報に二次情報識別データとインデックス情報を収めておくことで、情報の管理運用が柔軟にできる。

例えば様々なサービスプロバイダ（SP）が一次情報、または二次情報いずれかの管理主体となり、各SPは、それぞれの管理情報を顧客情報として、サービス提供対象となるユーザの個人識別証明書（IDC）と公開鍵証明書（PKC）のアクセスが可能となる。

#### 【0277】

上述のように、様々な態様で、個人識別証明書（IDC）と、該個人識別証明書の格納テンプレートの暗号化に適用した公開鍵の公開鍵証明書とを関連付けるリンクを構成したり、特定のサービスプロバイダ等データ通信先との接続処理の際の、個人認証、相互認証または暗号処理データ通信を実行する際に適用する個人識別との接続処理の際に適用する個人識別証明書と公開鍵証明書との組合わせについてのリンクを構成することで、一方の証明書から他方の証明書を導くことが容易となり、例えばテンプレートの暗号化、復号処理に適用する鍵を特定する処理や、サービスプロバイダに対する個人識別証明書を利用した個人認証の後に、公開鍵証明書を利用した相互認証を行なう場合等に、必要なデータを迅速に特定することが可能となる。

#### 【0278】

〔8. 個人識別証明書（IDC）による認証と公開鍵証明書（PKC）に基づくコンテンツ利用処理〕

次に、個人識別証明書（IDC）による個人認証を行ない、音楽データ、画像データ等のコンテンツをサービスプロバイダが受信（ダウンロード）する処理について、具体的に説明する。

#### 【0279】

これまでの説明から明らかなように、個人識別証明書による個人認証のためには、サンプリング情報とテンプレートの比較照合を実行し、その結果を出力するシステムが必要となる。ここでは、ユーザの使用するコンテンツ再生機器としてのユーザデバイスにサンプリング情報とテンプレートの比較照合処理を実行する機構を備え、照合結果に応じてサービスプロバイダに対するネットワークを介したコンテンツのダウンロード処理、あるいはサービスプロバイダに対するユーザ登録処理、契約処理、ユーザ登録抹消処理、さらに個人識別認証局（IDA）に

対する個人識別証明書（IDC）の発行要求処理を実行するシステム構成、および処理方法について説明する。

#### 【0280】

図53に個人認証を実行し、かつコンテンツ再生可能なユーザデバイスの構成を示す。ユーザデバイス500は、コンテンツ再生機構部501、コンテンツデータ蓄積部502、個人識別装置503、ネットワーク接続部504、公開鍵暗号処理部505、選択機能部506、入出力機能部507を有する。

#### 【0281】

コンテンツ再生機構部501は、コンテンツデータ蓄積部にあるデータを読み出し、再生する機能をもつ。コンテンツデータ蓄積部502は、コンテンツデータをネットワークを通じてダウンロードし、蓄える機能をもつ。個人識別装置503は、利用者から個人を識別するために必要な情報としてのサンプリング情報を入力し、デジタルデータに変換する機能と、変換したデジタルデータと、既登録デジタルデータであるテンプレートとの比較照合を実行する機能をもつ。ネットワーク接続部504は、ユーザデバイスとネットワークを接続する機能をもつ。公開鍵暗号処理部505は、指定されたデータに対して署名をつける機能と、指定された暗号データを復号する機能と、指定されたデータを暗号化する機能と、公開鍵と秘密鍵のペアを作成する機能と、任意の公開鍵証明書とあるデータのリンクを作る機能をもつ。公開鍵暗号処理部505はSAM（Secure Application Module）として構成されている。選択機能部506は、再生時にデータを選択する機能と、ネットワークに接続する時、接続先を選択する機能と、ダウンロード時にコンテンツのタイトルを選択する機能をもつ。入出力機能部507は、ユーザインターフェースを実現する。表示デバイスや入力デバイスをコントロールし、指定された情報を表示したり、利用者から入力された情報を処理可能なデータに変換する。

#### 【0282】

ここで、ユーザデバイス500の公開鍵暗号処理部505には、公開鍵証明書（PKC）、個人識別証明書（IDC）が格納されており、これらは相互にリンクされたデータ形式、すなわち、いずれかの証明書から他方の証明書を特定する

ことが可能なデータを有する構成である。具体的なリンク形態については、前述の〔個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンク〕の項目を参照されたい。ユーザは、公開鍵暗号処理部 5 0 5 に格納された個人識別証明書（IDC）により、個人認証を実行し、サービスプロバイダとの取り引きにおいて公開鍵証明書（PKC）を使用する。

## 【 0 2 8 3 】

## （コンテンツダウンロード処理）

上述の構成を持つユーザデバイスにおいて、サンプリング情報とテンプレートの比較照合処理の結果に基づいて、サービスプロバイダから音楽データ、画像データ等のコンテンツのダウンロードおよび再生を行なう処理について説明する。図 5 4 にコンテンツダウンロード処理におけるデータの流れを説明する図を示し、詳細処理フローを図 5 5，図 5 6，図 5 7 に示す。以下、これらの図を参照して処理を説明する。なお、以下の説明では、図 5 4 の番号を（n）、図 5 5～5 7 のステップ番号（S n n n）として示す。

## 【 0 2 8 4 】

まず、（1）デバイスを使うために、利用者は個人の指紋情報等のサンプリングデータをデバイスに入力する（S 3 0 1）。（2）個人識別装置は、入力されたサンプリングデータと、既に格納している個人識別証明書（IDC）内のテンプレートを比較するために、SAM に対して個人識別証明書（IDC）を要求する（S 3 0 2）。

## 【 0 2 8 5 】

次に、（3）リンク情報を使い、個人識別証明書（IDC）を検索し、IDC または IDC から抽出したテンプレートを個人識別装置に渡す（S 3 0 3～S 3 0 5）。（4）個人識別装置は、サンプリングデータとテンプレートの照合処理（S 3 0 6）を実行し、照合成立と判定し、個人認証成立と認められる利用者であると判断した場合、利用者とネットワーク接続部に対して個人認証成功を通知する（S 3 0 7，S 3 0 8）。この個人認証成立を条件として、ネットワーク接続部はネットワーク接続のための準備を行う（S 3 0 9）。

## 【 0 2 8 6 】

(5) 利用者は入出力機能部が提供するインターフェースを利用して、再生したいデータを指示・操作する (S 3 1 0, S 3 1 1)。(6) 選択機能部は、インターフェースを通して受け付けた指示を変換し、ネットワーク接続部への制御指示を生成 (S 3 1 1, S 3 1 2) し、制御指示をネットワーク接続部へ渡す (S 3 1 3)。

#### 【 0 2 8 7 】

次に、(7) ネットワーク接続部は、必要なコンテンツデータの取り引きにおいて必要となる公開鍵証明書 (PKC) を公開鍵暗号処理部に要求する (S 3 1 4 ~ S 3 1 6)。(8) 公開鍵暗号処理部は、要求された公開鍵証明書 (PKC) をネットワーク接続部に渡す (S 3 1 7)。なお、必要に応じて、公開鍵暗号処理部は IDC と PKC のリンクをたどり必要な PKC を探して、見つけた PKC をネットワーク接続部に渡す処理を実行する。

#### 【 0 2 8 8 】

次に、(9) ネットワーク接続部は、ローカルネットワークやインターネットを介して、コンテンツデータ提供サーバにアクセスする (S 3 1 8)。デバイスとサーバとの間で公開鍵証明書ベースの相互認証を行い、セッション鍵を共有するなどして、秘匿通信路を確保する (S 3 1 9)。図 5 4 に示す (9-1) ~ (9-8) は、サービス利用に関して、インタラクティブに利用者とサーバが情報交換を行う必要がある場合の処理で、必要な回数繰り返す (S 3 2 0, S 3 2 1)。コンテンツ提供サーバからのデータが (9-1) ~ (9-4) を介して利用者に送信され、ユーザからの送信データが (9-5) ~ (9-8) でコンテンツ提供サーバに流れる。このデータ送受信においては、必要に応じてセッションキーによる暗号化処理、それぞれの秘密鍵による署名処理、公開鍵による署名検証処理等のデータ検証処理を行なうことが好ましい。

#### 【 0 2 8 9 】

一連のデータのやり取りが終了すると、(10) ネットワーク接続部は、コンテンツ提供サーバから必要なコンテンツデータをダウンロードする (S 3 2 2)。次に、(11) ネットワーク接続部は、ダウンロードしたコンテンツデータをコンテンツデータ蓄積部に渡しコンテンツデータを保存し、(S 3 2 3) セッシ

ョンを終了する（S 3 2 4）。

#### 【0 2 9 0】

次に、（1 2）データ再生が利用者から要求されていた場合は、コンテンツデータをコンテンツ再生機構部に渡す（S 3 2 5でY e s）。（1 3）利用者は、コンテンツ再生機構部でコンテンツの再生を実行（S 3 2 6）し、入出力機能部を介して利用する。

#### 【0 2 9 1】

以上が、コンテンツのダウンロード、再生処理の流れである。ただし、上述した処理は、コンテンツのダウンロード時に公開鍵証明書（P K C）、個人識別証明書（I D C）の利用を行ない、かつその2つの証明書がS A M内部に格納されている順調な処理の流れである。図5 5～5 7の処理フローには、証明書がない場合、必要としない場合の処理についても示している。これらの処理について説明する。

#### 【0 2 9 2】

図5 6のステップS 3 2 8～S 3 3 2の処理は、ユーザデバイス内に対応する個人識別証明書（I D C）が検出されない場合の処理である。この場合、ユーザデバイスは、入出力機能部を介してI D Cが見つからない旨のメッセージを表示し（S 3 2 8）、I D Cの発行要求を実行するか否かをユーザに判断させ（S 3 2 9）、ユーザからの入力により発行要求を行なわないとされた場合は、ダウンロード失敗を利用者に通知する（S 3 3 2）。一方、利用者からの入力によりI D C発行要求を行なうとの意思表示がなされた場合は、コンテンツのダウンロード処理を終了し、I D C発行要求処理に移行することを入出力機能部を介して通知する（S 3 3 0）。その後、I D Cの発行処理を実行する（S 3 3 1）。この処理の詳細は、前述の「テンプレート、個人識別証明書（I D C）の登録、変更処理」の欄を参照されたい。

#### 【0 2 9 3】

図5 7のステップS 3 3 3以下は、公開鍵証明書（P K C）がユーザデバイスに保存されていない場合の処理を示している。公開鍵証明書（P K C）を外部機関である認証局（C A）から取得して受信することを望む場合（S 3 3 3）、既



に登録済みの公開鍵証明書（PKC）の有無を判定（S334）し、ある場合は、その公開鍵証明書（PKC）を認証局（CA）から取得してユーザデバイスに格納する（S335）。

#### 【0294】

登録済みの公開鍵証明書（PKC）が無い場合は、新規発行処理となり、公開鍵、秘密鍵の鍵ペアを生成して、公開鍵証明書（PKC）の発行機関であるRA（登録局）に対して新規発行要求を行なう（S336）。新規に公開鍵証明書（PKC）が発行された場合は、個人識別証明書（IDC）とのリンク情報としての組情報を生成して、公開鍵証明書を格納する（S338）。ただし、前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存する処理は必要とされない。

#### 【0295】

S339以下は、新規の公開鍵証明書（PKC）の発行が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介してダウンロード失敗を通知して処理を終了する。

#### 【0296】

（ユーザ登録、抹消、サービス契約処理）

次に、コンテンツの提供、商品販売、決済処理等の様々なサービスを提供するサービスプロバイダに対しての、ユーザ登録、ユーザ登録抹消、サービス契約処理等を図53に示すユーザデバイス、すなわちテンプレートとサンプリング情報との比較照合処理を実行する個人識別装置を有する構成での照合処理に基づいて実行する構成について説明する。図58にユーザ登録、ユーザ登録抹消、サービス契約処理におけるデータの流れを説明する図を示し、詳細処理フローを図59、図60、図61に示す。以下、これらの図を参照して処理を説明する。なお、以下の説明では、図58の番号を（n）、図59～61のステップ番号（Snnn）として示す。

#### 【0297】

まず、（1）デバイスを使うために、利用者は個人の指紋情報等のサンプリン

グデータをデバイスに入力する（S 4 0 1）。（2）個人識別装置は、入力されたサンプリングデータと、既に格納している個人識別証明書（IDC）内のテンプレートを比較するために、SAMに対して個人識別証明書（IDC）を要求する（S 4 0 2）。

## 【 0 2 9 8 】

次に、（3）リンク情報を使い、個人識別証明書（IDC）を検索し、IDCまたはIDCから抽出したテンプレートを個人識別装置に渡す（S 4 0 3～S 4 0 5）。（4）個人識別装置は、サンプリングデータとテンプレートの照合処理（S 4 0 6）を実行し、照合成立と判定し、個人認証成立と認められる利用者であると判断した場合、利用者とネットワーク接続部に対して個人認証成功を通知する（S 4 0 7, S 4 0 8）。この個人認証成立を条件として、ネットワーク接続部はネットワーク接続のための準備を行う（S 4 0 9）。

## 【 0 2 9 9 】

（5）利用者は入出力機能部が提供するインターフェースを利用して、処理に対応したデータ入力、すなわちユーザ登録であれば、希望登録サイト、ユーザ登録抹消であれば、抹消を希望するサイト、契約処理であれば契約を希望するサイト等のデータ入力を実行する（S 4 1 0）。（6）選択機能部は、インターフェースを通して受け付けた指示を変換し、ネットワーク接続部への制御指示を生成し、制御指示をネットワーク接続部へ渡す（S 4 1 1）。

## 【 0 3 0 0 】

次に、（7）ネットワーク接続部は、必要なコンテンツデータの取り引きにおいて必要となる公開鍵証明書（PKC）を公開鍵暗号処理部に要求する（S 4 1 2）。（8）公開鍵暗号処理部は、要求された公開鍵証明書（PKC）をネットワーク接続部に渡す（S 4 1 3～S 4 1 5）。なお、必要に応じて、公開鍵暗号処理部はIDCとPKCのリンクをたどり必要なPKCを探して、見つけたPKCをネットワーク接続部に渡す処理を実行する。

## 【 0 3 0 1 】

次に、（9）ネットワーク接続部は、ローカルネットワークやインターネットを介して、サービス登録サーバまたはユーザ登録サーバにアクセスする（S 4 1

6)。デバイスとサーバとの間で公開鍵証明書ベースの相互認証を行い、セッション鍵を共有するなどして、秘匿通信路を確保する（S417）。図58に示す（9-1）～（9-8）は、サービス利用に関して、インタラクティブに利用者とサーバが情報交換を行う必要がある場合の処理で、必要な回数繰り返す（S418, S419）。サービス登録サーバまたはユーザ登録サーバからのデータが（9-1）～（9-4）を介して利用者に送信され、ユーザからの送信データが（9-5）～（9-8）でサービス登録サーバまたはユーザ登録サーバに流れる。このデータ送受信においては、必要に応じてセッションキーによる暗号化処理、それぞれの秘密鍵による署名処理、公開鍵による署名検証処理等のデータ検証処理を行なうことが好ましい。

#### 【0302】

一連のデータのやり取りが終了すると、（10）ネットワーク接続部は、サービス登録サーバまたはユーザ登録サーバから必要なデータをダウンロードする（S420）。次に、（11）ネットワーク接続部は、処理（ユーザ登録、ユーザ登録抹消、契約処理等）が成功した場合に、公開鍵暗号処理部に処理成功を通知する。さらに、必要であれば、個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンク情報（組情報）に必要な情報を追加する（S422, 423）。前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存する処理は必要とされない。（12）これらの処理が終了すると、処理結果を入出力機能部を介して表示して処理を終了する（S424, S425）。

#### 【0303】

以上が、ユーザ登録、ユーザ登録抹消、サービス契約等、サービスプロバイダとの対応において、個人識別証明書（IDC）を適用して個人認証処理を実行する場合の処理の流れである。ただし、上述した処理は公開鍵証明書（PKC）、個人識別証明書（IDC）の利用を行ない、かつその2つの証明書がSAM内部に格納されている順調な処理の流れである。図60～62の処理フローには、証明書がない場合、必要としない場合の処理についても示している。これらの処理について説明する。

## 【0304】

図60のステップS426～S430の処理は、ユーザデバイス内に対応する個人識別証明書（IDC）が検出されない場合の処理である。この場合、ユーザデバイスは、入出力機能部を介してIDCが見つからない旨のメッセージを表示し（S426）、IDCの発行要求を実行するか否かをユーザに判断させ（S427）、ユーザからの入力により発行要求を行なわないとされた場合は、処理失敗を利用者に通知する（S430）。一方、利用者からの入力によりIDC発行要求を行なうとの意思表示がなされた場合は、コンテンツのダウンロード処理を終了し、IDC発行要求処理に移行することを入出力機能部を介して通知する（S428）。その後、IDCの発行処理を実行する（S429）。この処理の詳細は、前述の〔テンプレート、個人識別証明書（IDC）の登録、変更処理〕の欄を参照されたい。

## 【0305】

図61のステップS431以下は、公開鍵証明書（PKC）がユーザデバイスに保存されていない場合の処理を示している。公開鍵証明書（PKC）を外部機関である認証局（CA）から取得して受信することを望む場合（S431）、既に登録済みの公開鍵証明書（PKC）の有無を判定（S432）し、ある場合は、その公開鍵証明書（PKC）を認証局（CA）から取得してユーザデバイスに格納する（S433）。

## 【0306】

登録済みの公開鍵証明書（PKC）が無い場合は、新規発行処理となり、公開鍵、秘密鍵の鍵ペアを生成して、公開鍵証明書（PKC）の発行機関であるRA（登録局）に対して新規発行要求を行なう（S434）。新規に公開鍵証明書（PKC）が発行された場合は、個人識別証明書（IDC）とのリンク情報としての組情報を生成して、公開鍵証明書を格納する（S436）。ただし、前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存する処理は必要とされない。

## 【0307】

ステップ S 4 3 7、S 4 3 8 は、ユーザ登録、ユーザ登録抹消、サービス契約等の各種処理が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介して処理失敗を通知して処理を終了する。また、ステップ S 4 3 9、S 4 4 0 は、新規の公開鍵証明書（PKC）の発行が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介して処理失敗を通知して処理を終了する。

#### 【0308】

（デバイスに格納する個人識別証明書（IDC）の要求、登録処理）

次に、図 5 3 に示すような個人識別装置を有するユーザデバイスに格納する個人識別証明書（IDC）の発行、登録処理手続きについて説明する。図 6 2 にデバイスに格納する個人識別証明書（IDC）の要求処理におけるデータの流れを説明する図を示し、詳細処理フローを図 6 3、図 6 4、図 6 5 に示す。以下、これらの図を参照して処理を説明する。なお、以下の説明では、図 6 2 の番号を（n）、図 6 3～6 5 のステップ番号（S n n n）として示す。

#### 【0309】

まず、（1）デバイスを使うために、利用者は個人の指紋情報等のサンプリングデータをデバイスに入力する（S 5 0 1）。（2）個人識別装置は、入力されたサンプリングデータと、既に格納している個人識別証明書（IDC）内のテンプレートを比較するために、SAM に対して個人識別証明書（IDC）を要求する（S 5 0 2）。なお、ここでは、ユーザデバイスに発行済みの個人識別証明書（IDC）が n 個存在し、さらに新たなテンプレートを格納した個人識別証明書（IDC）の発行を要求する処理を行なうものとする。デバイスに個人識別証明書（IDC）が全く存在しない場合は、n = 0 とした処理となる。

#### 【0310】

ユーザデバイスは、（3）格納済みの n 個の個人識別証明書（IDC）を、順次検索し、IDC または IDC から抽出したテンプレートを個人識別装置に渡す（S 5 0 3～S 5 0 5）。（4）個人識別装置は、サンプリングデータとテンプレートの照合処理（S 5 0 6）を実行し、照合成立と判定し、個人認証成立と認められる利用者であると判断した場合、利用者に対して個人認証成功を通知する

(S 5 0 7, S 5 0 8)。ただし、ここでの処理は、新たなテンプレートを持つ個人識別証明書 (I D C) の発行を要求するものであり、サンプリングデータと一致する個人識別証明書 (I D C) は格納されていないとする。すべての格納 I D C と照合しても一致するテンプレートを格納した I D C が見つからない場合、ステップ S 5 0 9 に進む。

#### 【 0 3 1 1 】

ユーザデバイス内にサンプリング情報と一致するテンプレートを持つ個人識別証明書 (I D C) が検出されない場合、ユーザデバイスは、入出力機能部を介して I D C が見つからない旨のメッセージを表示 (S 5 0 9) し、I D C の発行要求を実行するか否かをユーザに判断させ (S 5 1 0)、ユーザからの入力により発行要求を行なわないとされた場合は、処理終了を利用者に通知する (S 5 1 2)。一方、利用者からの入力により I D C 発行要求を行なうとの意思表示がなされた場合は、I D C 発行要求処理に移行することを入出力機能部を介して通知する (S 5 1 1)。

#### 【 0 3 1 2 】

図 6 4 に示すステップ S 5 1 3 以下の処理は、個人識別証明書 (I D C) の発行処理において使用する公開鍵証明書 (P K C) の発行処理フローである。

#### 【 0 3 1 3 】

ステップ S 5 1 3 では、個人識別証明書 (I D C) の発行処理に公開鍵証明書 (P K C) が必要か否かを判定し、必要である場合は、ステップ S 5 1 4 で、ユーザデバイスの公開鍵暗号処理部に格納された I D C、P K C またはリンク (組) 情報から公開鍵証明書 (P K C) の識別番号を取得する。公開鍵証明書 (P K C) が存在した場合 (S 5 1 6 で Y e s) は、(9) 公開鍵証明書 (P K C) を公開鍵暗号処理部に渡し (S 5 1 6)、I D R A (個人識別証明書 (I D C) を発行する登録局) への接続準備を行い (S 5 1 7)、個人識別証明書 (I D C) の発行に必要な情報を入力する (S 5 1 8)。

#### 【 0 3 1 4 】

公開鍵証明書 (P K C) を外部機関である認証局 (C A) から取得して受信することを望む場合 (S 5 2 0)、既に登録済みの公開鍵証明書 (P K C) の有無

を判定（S 5 2 1）し、ある場合は、その公開鍵証明書（PKC）を認証局（CA）から取得してユーザデバイスに格納する（S 5 2 2）。

#### 【0 3 1 5】

登録済みの公開鍵証明書（PKC）が無い場合は、新規発行処理となり、公開鍵、秘密鍵の鍵ペアを生成（図 6 2（5））して、公開鍵証明書（PKC）の発行機関である RA（登録局）に対して新規発行要求（図 6 2（6）（7））を行なう（S 5 2 3）。新規に公開鍵証明書（PKC）が発行（図 6 2（8））された場合（S 5 2 4 で Yes）は、個人識別証明書（IDC）とのリンク情報としての組情報を生成して、公開鍵証明書を格納する（S 5 2 5）。ただし、前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存する処理は必要とされない。

#### 【0 3 1 6】

図 6 5 に示す処理は、IDRA（個人識別証明書（IDC）の発行登録受付をする登録局）との接続により、個人識別証明書（IDC）の発行を行なう処理である。

#### 【0 3 1 7】

（1 0）ユーザデバイスの公開鍵暗号処理部は、ネットワーク接続部へ公開鍵証明書とリンクする個人識別証明書（IDC）を獲得するために、IDRA のアドレスとサンプリングデータ（あるいは利用者名）を渡す。個人識別証明書（IDC）発行に必要なオフライン手続きは予め済ましてあるとする。IDRA が要求者の IDC を検索するため使用するオフライン手続きで登録した情報（各種個人情報）と照合するための情報（サンプリングデータ、PIN、氏名など）が別に必要ならば同時にネットワーク接続部へ渡す。

#### 【0 3 1 8】

（1 1）ユーザデバイスのネットワーク接続部は、ローカルネットワークやインターネットを介して、IDRA にアクセスする（S 5 2 6）。デバイスと IDRA との間で公開鍵証明書ベースの相互認証を行い、セッション鍵を共有するなどして、秘匿通信路を確保する（S 5 2 7）。ユーザデバイスは、必要な情報（

サンプリングデータ、PIN、氏名、住所、電話番号など）もIDRAに対して送信する。図62の（11）-1～8は、ユーザとIDRA間でのインタラクティブな通信処理を示す。（11）-1～4はIDRAがユーザにデータを送る場合、（11）-5～8はユーザがIDRAへデータを送る場合を示す。このデータ送受信においては、必要に応じてセッションキーによる暗号化処理、それぞれの秘密鍵による署名処理、公開鍵による署名検証処理等のデータ検証処理を行なうことが好ましい。発行される個人識別証明書（IDC）がユーザデバイスの公開鍵で暗号化したテンプレートを格納する場合には、ユーザデバイスからIDRAに対して公開鍵（公開鍵証明書）を送付する。

#### 【0319】

一連のデータのやり取りが終了すると、ネットワーク接続部は、必要なデータ、IDC発行要求の結果をダウンロードする（S530）。（12）IDRAは、ユーザデバイスから受信したIDC発行要求を検討し、正当な発行依頼であると判定すると、IDCの発行手続きを実行するIDCAに対してIDCの発行要求を行ない、IDCAによって発行された個人識別証明書（IDC）がIDRAを介してユーザデバイスに送信される。

#### 【0320】

（13）個人識別証明書（IDC）を受信したユーザデバイスは、個人識別証明書（IDC）を公開鍵暗号処理部に送信し、（14）公開鍵暗号処理部は個人識別証明書（IDC）と公開鍵証明書（PKC）のリンク情報としてのリンク（組）情報を生成（S532）して、リンク（組）情報の更新を実行する（S533）。ただし、前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存する処理は必要とされない。これらの処理が終了すると、（15）IDC発行要求処理の結果を入出力機能部を介して表示して処理を終了する（S534，S535）。

#### 【0321】

ステップS536、S537は、個人識別証明書（IDC）の発行処理が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介して



処理失敗を通知して処理を終了する。また、ステップ S 5 3 8, S 5 3 9 は、新規の公開鍵証明書（PKC）の発行が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介して処理失敗を通知して処理を終了する。

#### 【 0 3 2 2 】

#### 〔 9. ワンタイム公開鍵証明書（ワンタイム PKC） 〕

次に、個人識別認証局（IDA）のテンプレートを用いた個人認証に基づいて、認証局（CA）が、公開鍵証明書（PKC）を発行する処理形態について説明する。以下、この形態で発行される公開鍵証明書をワンタイム PKC と呼ぶ。ワンタイム PKC は、例えば取引のないサービスプロバイダとの間において、コンテンツ取得等の取引を行ないたい場合に、既に個人識別認証局（IDA）に登録されている個人識別証明書（IDC）に基づいて個人認証を実行し、認証局（CA）による厳格な審査手続きを省略した形で発行される公開鍵証明書である。正式な公開鍵証明書の位置づけとはならず、特定の取り引き、例えば 1 回限りの取り引きにおいて有効とみなされる公開鍵証明書である。

#### 【 0 3 2 3 】

図 6 6 にワンタイム PKC の発行手順を説明する図を示す。図中の番号順に処理が進行する。図 6 7 は、詳細なワンタイム PKC の発行手順を示すフロー図である。図 6 6, 6 7 に基づいてワンタイム PKC の発行処理を説明する。

#### 【 0 3 2 4 】

まず、ワンタイム PKC の発行要求を持つユーザは、認証要求装置に指紋データ等のサンプリングデータを入力（図 6 7, S 2 0 1）する。認証要求装置は、機器内で、サンプリングデータを入力したユーザの公開鍵、秘密鍵のペアをワンタイム PKC 用の鍵セットとして生成する（S 2 0 2）。

#### 【 0 3 2 5 】

次に、認証要求装置は、個人識別認証局（IDA）との間で相互認証処理を実行し（S 2 0 3）、認証成立を条件として、サンプリングデータ、生成した公開鍵、ユーザ識別データを送信する。送信データは、セッションキーで暗号化を行ない、さらに署名処理を実行して送付することが望ましい。

#### 【 0 3 2 6 】

認証要求装置からデータを受信した個人識別認証局（IDA）は受信サンプリングデータと、ユーザ識別データから識別されるユーザの予め登録済みの個人識別証明書（IDC）からテンプレートを抽出して、照合処理を実行する（S205）。次に、個人識別認証局（IDA）は、データベースからユーザIDを取り出し（S206）、個人識別認証局（IDA）と認証局（CA）との間で相互認証処理を実行し（S207）、認証成立を条件として、認証局（CA）にユーザIDと公開鍵を送信する（S208）。この場合の送信データについても暗号化、署名処理がなされることが望ましい。

#### 【0327】

認証局（CA）は、受信した公開鍵に対応する公開鍵証明書をワнтаイムPKCとして生成し、発行履歴を管理する（S209, 210）する。認証局（CA）は、生成したワнтаイムPKCを個人識別認証局（IDA）を介して認証要求装置に送付する（S211）。

#### 【0328】

認証要求装置は、受信したワнтаイムPKCを用い、例えばサービスプロバイダに対するサービスリクエストを実行する（S212, 213）。具体的には、例えばコンテンツ要求データ、あるいは決済要求データ等の要求データに生成した秘密鍵による署名を付加し、公開鍵証明書（ワнтаイムPKC）と併せてサービスプロバイダに送信する。

#### 【0329】

サービスプロバイダは、受信データから公開鍵証明書（ワнтаイムPKC）を取り出し、ユーザの公開鍵を抽出して、公開鍵を用いて署名検証を実行し、サービスリクエスト検証処理を行なう（S214）。検証がOKであれば、サービスを提供する（S215）。サービスを受領した認証要求装置は、装置内で生成した公開鍵、秘密鍵、および発行されたワнтаイムPKCの削除（S216）を行なう。なお、公開鍵、秘密鍵は削除せず、公開鍵証明書であるワнтаイムPKCのみを削除する処理構成としてもよい。

#### 【0330】

図67に示す一連の処理、すなわち、S201のサンプリングデータ送信から

、S 2 1 6 のデータ削除処理までの処理は、一連の処理を自動的に実行する特定の処理プログラム、例えばサービスプロバイダによって提供されるプログラムに基づいて実行される。従って、個人認証要求装置に送信されてきたワンタイム P K C は、処理の完結により個人認証要求装置から削除され、P K C の他の取り引きにおける流用が防止されるものとなっている。ただし、必ずしも削除処理を要求されるものではなく、特定の限定された取り引きにおいて、ワンタイム P K C を繰り返し使用可能とする形態としてもよい。

#### 【 0 3 3 1 】

このように、公開鍵証明書（ワンタイム P K C）の発行要求者の個人識別データとしてのテンプレートを個人識別証明書から取得し、テンプレートとサンプリング情報との照合処理により個人認証を実行し、個人認証の成立を条件として、要求者の公開鍵証明書を発行する構成としたので、公開鍵証明書の発行手続きが簡素化され、迅速な公開鍵証明書発行処理が可能となる。

#### 【 0 3 3 2 】

さらに、個人認証処理を個人識別認証局において実行し、公開鍵証明書（ワンタイム P K C）を発行する認証局においては、個人識別認証局の個人認証の成立を条件として公開鍵証明書を発行することが可能となるので、認証局における個人確認処理負担が軽減される。

#### 【 0 3 3 3 】

さらに、個人識別認証局によるユーザサンプリング情報と個人識別証明書の格納テンプレートとの照合処理による個人認証成立を条件として、ユーザに対して発行される公開鍵証明書（ワンタイム P K C）は、公開鍵証明書（ワンタイム P K C）を受領した情報処理装置における公開鍵証明書の利用処理完了に伴い削除処理が実行されるので、個人識別認証局の個人認証に基づく公開鍵証明書（ワンタイム P K C）特有の処理においてのみ利用可能な構成が実現される。

#### 【 0 3 3 4 】

#### [ 1 0 . 照合証明書 ]

個人識別認証局（I D A）は、個人識別証明書のテンプレートとサンプリング情報との照合により、両データが一致した場合は、サンプリング情報を提供した

個人が個人識別証明書に対応する個人であることを認証する。これまでに説明した例では、照合の結果について照合OKまたはNGの通知を行なうものとして説明してきたが、個人識別認証局（IDA）は、認証したことを示す証明書として照合証明書を発行する構成としてもよい。以下、照合証明書の発行処理について説明する。

#### 【0335】

図68に、照合証明書の第1の利用形態を説明する図を示す。図中の番号1～10の順で処理が進行する。さらに、細かく手続きを説明したフローを図69に示す。図68、69を用いて処理を説明する。

#### 【0336】

まず、個人認証処理を行なおうとするユーザは、サンプリングデータを個人認証要求装置に送信する（図69，S101）。ここでの個人認証要求装置は、例えばユーザデバイスまたは、サービスプロバイダの通信可能なシステムである。

#### 【0337】

次に、個人認証要求装置は、個人識別認証局（IDA）との間で相互認証処理を実行（S102）し、認証成立を条件として個人認証要求装置はサンプリングデータと個人認証要求装置の識別子（ID）を個人識別認証局（IDA）に送信（S103）する。この際のデータ送信は、認証処理において生成したセッションキー、あるいは個人識別認証局（IDA）の公開鍵で暗号化して送信する。認証が不成立の場合は、エラー処理（S122）とし、以下の処理は実行しない。

#### 【0338】

次に、個人識別認証局（IDA）は、自己のデータベースに格納されている認証対象者の個人識別証明書（IDC）のテンプレートを取り出して、受信したサンプリングデータとの照合を実行（S104）する。照合が不一致であった場合は、以下の手続きは実行されない。

#### 【0339】

次に、個人識別認証局（IDA）は、自己のデータベースに格納されている認証対象者の識別子（ID）を取り出し（S105）、照合の成立した個人のIDに基づいて照合証明書を生成する（S106）。さらに、照合証明書の発行履歴

、例えば証明書の発行日時、有効期間管理データを生成して格納する（S 1 0 7）。その後、個人識別認証局（IDA）は、照合証明書を、個人認証要求装置に対して発行する。

#### 【0 3 4 0】

以下の処理は、発行された照合証明書を利用してサービスプロバイダに対してサービス提供の要求を行なう場合の処理である。照合証明書の発行を受けたユーザは、照合証明書と、サービス要求データ等の電文に署名を付加し、さらに、公開鍵証明書を添付してサービスリクエストをサービスプロバイダに対するリクエストとして生成（S 1 0 9）し、サービスプロバイダに対して送信する（S 1 1 0）。

#### 【0 3 4 1】

サービスプロバイダは、受信した公開鍵証明書から、公開鍵を取り出して、署名を検証し（S 1 1 1）、データ改竄のないことを条件として、ユーザにサービスを提供する（S 1 1 2）。さらに、サービスを受信した個人認証要求装置は、照合証明書を削除する（S 1 1 3）。

#### 【0 3 4 2】

図 6 9 に示す一連の処理、すなわち、S 1 0 1 のサンプリングデータ送信から、S 1 1 3 の照合証明書削除処理までの処理は、一連の処理を自動的に実行する特定の処理プログラム、サービスプロバイダによって提供されるプログラムに基づいて実行される。従って、個人認証要求装置に送信されてきた照合証明書は、処理の完結により個人認証要求装置から削除され、証明書の流用が防止されるものとなっている。ただし、必ずしも削除処理を要求されるものではなく、例えば特定の限定された取り引きにおいて、照合証明書を繰り返し使用可能とする形態としてもよい。

#### 【0 3 4 3】

図 7 0 に示す照合証明書利用態様（2）は、図 6 8 の例と異なり、サービスプロバイダが、サービス提供ユーザの照合証明書を取得する処理構成である。

#### 【0 3 4 4】

サービスプロバイダに対してサービス提供を要求するユーザは、認証要求装置

において、サービスリクエストおよび指紋データ等のサンプリングデータを構成要素とするリクエストデータを生成し、署名を実行する。次に、認証要求装置とサービスプロバイダ間で相互認証を実行し、認証成立を条件として、生成リクエストデータを送信する。

#### 【0345】

リクエストデータを受信したサービスプロバイダは、署名を検証して、データ改竄チェックを実行し、改竄のないことを確認の後、個人識別認証局（IDA）との間で相互認証処理を実行し、ユーザから受信したサンプリングデータと認証要求装置のIDを、サービスプロバイダの署名を付けて送信する。

#### 【0346】

個人識別認証局（IDA）は、受信データの検証を行ない、データ改竄のないことを確認して、受信サンプリングデータとテンプレートとの照合処理を実行し、照合成立を条件として照合証明書を生成し、発行履歴を生成、格納する。

#### 【0347】

生成した照合証明書は、サービスプロバイダに送付され、サービスプロバイダは照合証明書により、サービス要求ユーザの認証がなされたとの判定を行ない、認証要求装置、ユーザに対してサービス提供のOKを通知する。サービスプロバイダは、照合証明書を削除して処理を終了する。

#### 【0348】

図71に照合証明書のフォーマット例を示す。各データ項目について説明する。

#### 【0349】

バージョン（version）は、照合証明書フォーマットのバージョンを示す。

認証番号（Serial Number）は、個人識別認証局（IDA）によって設定される各照合証明書のシリアルナンバである。

署名方式（Signature algorithm Identifier algorithm parameter）は、照合証明書の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびRSAがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、RSAが適用されて

いる場合には鍵長が記録される。

発行者 (issuer) は、照合証明書の発行者、すなわち個人識別認証局 (IDA) の名称が識別可能な形式 (Distinguished Name) で記録されるフィールドである。

有効期限 (validity) は、証明書の有効期限である開始日時、終了日時が記録される。

サブジェクト (subject) は、ユーザである認証対象者の名前が記録される。具体的には例えばユーザの ID や、氏名等である。

個人識別証明書情報 (Subject IDA Info) は、ユーザの個人識別証明書情報として、例えば個人識別証明書の認証番号、認証者固有 ID 等の各情報が格納される。

公開鍵証明書情報 (Subject PKC info) には、被認証者の公開鍵証明書情報としての、被認証者の公開鍵証明書の認証番号、被認証者の公開鍵証明書の被認証者固有 ID が格納される。

電子署名は、証明書を構成する各フィールドの全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して個人識別認証局 (IDA) の秘密鍵を用いて生成したデータである。

#### 【 0 3 5 0 】

上述のように、照合証明書には、公開鍵証明書、個人識別証明書とリンクが張れるように、公開鍵証明書情報、個人識別証明書情報が含まれている。また、被認証者識別データが含まれている。

#### 【 0 3 5 1 】

[ 1 1. 個人識別証明書 (IDC) のダウンロードおよびコンテンツ利用処理]

次に、ユーザの個人識別証明書 (IDC) が格納されていないデバイスを使用してコンテンツの配信等の際に、個人識別認証局 (IDA) に登録済みの個人識別証明書 (IDC) を利用して個人認証を実行し、コンテンツ配信等のサービスを受ける処理について説明する。

#### 【 0 3 5 2 】

音楽データ、画像データ等の様々なコンテンツをサービスプロバイダから受信しようとするユーザは、1つのユーザ端末（ユーザデバイス）を使用するとは限らず、複数のデバイスを使用する場合がある。例えば自宅のデバイス、会社のデバイス、あるいは不特定多数が利用可能なデバイス等である。

## 【0353】

上述した個人識別証明書（IDC）を使用した個人認証を実行するためには、個人識別証明書に対するアクセスが必要となる。例えばユーザAが頻繁に利用するユーザデバイスに個人識別証明書（IDC）が格納されていれば、その格納IDCを用いて個人認証がそのデバイスにおいて実行可能であるが、会社のデバイス、あるいは不特定多数が利用可能なデバイスに、そのデバイスを利用するすべてのユーザの個人識別証明書（IDC）を格納することは現実的でない。このような状況にあるデバイスにおいて、個人識別認証局（IDA）に登録済みの個人識別証明書（IDC）を利用して個人認証を行ない、さらにその個人認証処理に基づいてコンテンツ配信を受ける処理について、以下説明する。

## 【0354】

図72に、個人識別認証局（IDA）に登録済みの個人識別証明書（IDC）を利用して個人認証を行ない、さらに、個人認証処理に基づいてコンテンツ配信を受ける処理を説明する図を示す。図中の番号1～11の順で処理が進行する。さらに、詳細な手続きを説明したフローを図73～図75に示す。図72、および図73～図75を用いて処理を説明する。

## 【0355】

図72に示すように、ユーザAは、通常は、ユーザAのデバイスAを用いて処理、例えばコンテンツの受信等の処理を実行する。従ってデバイスAには、コンテンツの配信を実行するために必要な各種の証明書、すなわちユーザAの公開鍵証明書（PKC）、個人識別証明書（IDC）、さらに、デバイスAの公開鍵証明書（PKC）が格納されている。ユーザAは必要に応じて、各種PKCを用いて相互認証処理を実行し、また、IDCを用いて個人認証処理が実行可能である。

## 【0356】



ここで、ユーザAが、他のデバイス、図72に示す例では、ユーザBのデバイスBを使用してコンテンツ配信等のサービスを受ける場合を考える。デバイスBには、ユーザBの公開鍵証明書（PKC）、個人識別証明書（IDC）、さらに、デバイスBの公開鍵証明書（PKC）が格納されている。ユーザBは、これらの証明書を利用して相互認証、個人認証処理が実行可能であるが、ユーザAは、デバイスBに格納された各証明書のみでは、個人認証、または相互認証が実行できない場合がある。このようなデバイスBにおいてユーザAがIDCを利用した個人認証、PKCを利用した相互認証を実行してコンテンツの配信サービスを実行する処理を図73以下のフローを用いて説明する。

#### 【0357】

まず、デバイスBを利用するユーザAは、デバイスBにアクセス（起動）する（S801）。デバイスBは、デバイスBに対するアクセス許可のあるユーザによるアクセスであるか否かを判定するために、個人認証処理を開始（S802）し、ユーザAに対してサンプリング情報の入力を要求する。ユーザAは、デバイスBにユーザIDと指紋等のサンプリング情報を入力（S803）すると、デバイスBは、ユーザID、またはサンプリング情報に基づいてデバイス内の記憶手段の格納IDCの検索を実行（S804）する。デバイスBには、ユーザAに対応するIDCは格納されていないので、IDCは検出されない。この場合、デバイスBは、ユーザAのIDCを個人識別認証局（IDA）に要求する。この際、デバイスBは、個人識別認証局（IDA）との間で相互認証を実行し、セッションキーを生成してセッションキーによる暗号化を行なったユーザAのユーザID、サンプリング情報を個人識別認証局（IDA）に送信する。

#### 【0358】

次に、個人識別認証局（IDA）は、自己のデータベースに格納されているユーザAの個人識別証明書（IDC）を取り出して、デバイスBに送信する。なお、この場合、個人識別証明書（IDC）内に格納するテンプレート情報は、デバイスBにおいて利用可能な形態、具体的にはデバイスBの公開鍵で暗号化してIDCに格納する。デバイスBは受信したユーザAの個人識別証明書（IDC）をデバイス内のメモリに格納する（S806）。

## 【 0 3 5 9 】

デバイスBは、メモリに格納したユーザAの個人識別証明書（IDC）を用いてサンプリングデータとの照合を実行、すなわち個人認証処理を行なう（S 8 0 7）。照合が不一致であった場合は、エラーとなり、以下の手続きは実行されない。

## 【 0 3 6 0 】

個人認証が成立すると、デバイスBは、サービスプロバイダの提供するサービスに適用可能な公開鍵・秘密鍵のペアを検索（S 8 0 9）する。なお、サービスプロバイダは、各ユーザとの間のデータ通信において、予め各ユーザ毎、あるいはデバイス毎に設定された公開鍵・秘密鍵のペアを用いて相互認証等、各種の暗号化処理を実行するものとする。ここでは、ユーザA専用の公開鍵・秘密鍵のペアは、デバイスBに格納されておらず、ステップS 8 1 0の判定はNoとなり、デバイスBにおいて、新たな公開鍵・秘密鍵のペアを生成する（S 8 1 1）。

## 【 0 3 6 1 】

次にデバイスBは、生成した公開鍵を認証局（CA）に送信し、公開鍵証明書の発行手続きを実行して、ユーザAの公開鍵証明書（PKC）を取得し、デバイスBに格納する（S 8 1 2）。

## 【 0 3 6 2 】

次に、デバイスBは、ユーザAの個人識別証明書（IDC）と、公開鍵証明書（PKC）のリンクを形成する。リンクは例えば前述の組情報を生成してメモリに格納する処理として実行する。この際、リンク（組情報）に対してそのIDC，PKCを適用して利用可能なサービス名を対応付けて登録する（S 8 1 3）。すなわち、いずれのサービスプロバイダまたはコンテンツプロバイダからのサービスに適用可能なIDC，PKCセットであるかを対応付けて、例えばプロバイダ識別子またはサービス識別子等の処理識別子を併せて登録する。

## 【 0 3 6 3 】

次に、デバイスBは、ユーザAの公開鍵証明書（PKC）を用いて、サービス登録サーバと相互認証を実行（S 8 1 4）する。なお、サービス登録サーバは、管轄する1以上のサービスプロバイダ（コンテンツ配信サーバ等）のサービスを

提供するユーザのユーザ登録を行なうサーバであり、各ユーザの公開鍵証明書（PKC）を登録することにより、管轄下のサービスプロバイダのサービス実行時の認証処理等、各種暗号処理を登録PKCを用いて実行可能としたサーバである。

#### 【0364】

サービス登録サーバとの相互認証が成立すると、次にサービス登録サーバに対するユーザAの個人認証をユーザAの個人識別証明書（IDC）を用いて実行する（S816）。これらの処理が済むと、サービス登録サーバは、ユーザAの公開鍵証明書（PKC）を登録（S818）する。なお、個人認証処理は必要に応じて実行すればよく、必須ではない。例えばコンテンツ配信時にコンテンツ配信サーバとの間で個人認証を行なってもよい。

#### 【0365】

デバイスBは、サービス登録サーバからユーザAの公開鍵証明書（PKC）の登録終了通知を受領し、登録したユーザAの公開鍵証明書（PKC）を用いて利用可能なサービス情報、コンテンツ配信サーバのPKCを受信（S819）する。

#### 【0366】

以下の処理は、コンテンツ配信サーバからのコンテンツ配信を実行する処理であり、ステップS820でコンテンツ配信サーバのPKCとユーザAのPKCとを用いて、相互認証処理を実行し、相互認証の成立を条件としてコンテンツの配信を受ける（S822）。なお、コンテンツ配信サーバは、デバイスBからのコンテンツ要求に応じて、コンテンツ要求の際の相互認証に用いられたPKCがコンテンツ利用権のあるPKCとしてサービス登録サーバに登録されているか否かを確認する処理を実行する。確認が取れた場合にのみコンテンツの配信を行なう。サービス登録サーバには、ユーザAの公開鍵証明書（PKC）が登録済みであるので、コンテンツ要求は承認され、コンテンツが配信されることになる。

#### 【0367】

このように、デバイスに、ユーザの個人識別証明書（IDC）、公開鍵証明書（PKC）が格納されていない場合であっても、ユーザは、個人識別認証局（I

DA) に登録された IDC をデバイスにダウンロードし、さらにデバイスにおいて生成した公開鍵・秘密鍵のペアに基づいて認証局 (CA) から公開鍵証明書 (PKC) を受領し、IDC に基づく個人認証、PKC に基づく相互認証、データ暗号化処理を実行し、サービスプロバイダからのサービス提供を受領することが可能となる。

#### 【0368】

以上が、ユーザ個人に対して設定された個人識別証明書 (IDC)、公開鍵証明書 (PKC) を用いた処理である。次にユーザ個人に対して設定された個人識別証明書 (IDC) と、デバイスに対して設定された公開鍵証明書 (PKC) を用いた処理について説明する。

#### 【0369】

図 7 6 に、ユーザ個人に対して設定された個人識別証明書 (IDC) と、デバイスに対して設定された公開鍵証明書 (PKC) を用い、個人識別認証局 (IDA) に登録済みの個人識別証明書 (IDC) を利用して個人認証を行ない、デバイスに対して設定された公開鍵証明書 (PKC) に基づいてコンテンツ配信を受ける処理を説明する図を示す。図中の番号 1 ～ 6 の順で処理が進行する。さらに、詳細な手続きを説明したフローを図 7 7 ～ 図 7 8 に示す。図 7 6、および図 7 7 ～ 図 7 8 を用いて処理を説明する。

#### 【0370】

図 7 6 に示すように、ユーザ A は、通常は、ユーザ A のデバイス A を用いて処理、例えばコンテンツの受信等の処理を実行する。従ってデバイス A には、コンテンツの配信を実行するするために必要な各種の証明書、すなわちユーザ A の公開鍵証明書 (PKC)、個人識別証明書 (IDC)、さらに、デバイス A の公開鍵証明書 (PKC) が格納されている。ユーザ A は必要に応じて、各種 PKC を用いて相互認証処理を実行し、また、IDC を用いて個人認証処理が実行可能である。

#### 【0371】

ここで、ユーザ A が、他のデバイス、図 7 6 に示す例では、ユーザ B のデバイス B を使用してコンテンツ配信等のサービスを受ける場合を考える。デバイス B

には、ユーザBの個人識別証明書（IDC）、さらに、デバイスBの公開鍵証明書（PKC）が格納されている。ユーザBは、これらの証明書を利用して相互認証、個人認証処理が実行可能であるが、ユーザAは、デバイスBに格納された各証明書のみでは、個人認証が実行できない。このようなデバイスBにおいてユーザAがIDCを利用した個人認証、PKCを利用した相互認証を実行してコンテンツの配信サービスを実行する処理を図77以下のフローを用いて説明する。

#### 【0372】

まず、デバイスBを利用するユーザAは、デバイスBにアクセス（起動）する（S851）。デバイスBは、デバイスBに対するアクセス許可のあるユーザによるアクセスであるか否かを判定するために、個人認証処理を開始（S852）し、ユーザAに対してサンプリング情報の入力进行を要求する。ユーザAは、デバイスBにユーザIDと指紋等のサンプリング情報を入力（S853）すると、デバイスBは、ユーザID、またはサンプリング情報に基づいて格納IDCの検索を実行（S854）する。デバイスBには、ユーザAに対応するIDCは格納されていないので、IDCは検出されない。この場合、デバイスBは、ユーザAのIDCを個人識別認証局（IDA）に要求する。この際、デバイスBは、個人識別認証局（IDA）との間で相互認証を実行し、セッションキーを生成してセッションキーによる暗号化を行なったユーザAのユーザID、サンプリング情報を個人識別認証局（IDA）に送信する。

#### 【0373】

次に、個人識別認証局（IDA）は、自己のデータベースに格納されているユーザAの個人識別証明書（IDC）を取り出して、デバイスBに送信する。なお、この場合、個人識別証明書（IDC）内に格納するテンプレート情報は、デバイスBにおいて利用可能な形態、具体的にはデバイスBの公開鍵で暗号化してIDCに格納する。デバイスBは受信したユーザAの個人識別証明書（IDC）をデバイス内のメモリに格納する（S856）。

#### 【0374】

デバイスBは、メモリに格納したユーザAの個人識別証明書（IDC）を用いてサンプリングデータとの照合を実行、すなわち個人認証処理を行なう（S85

7)。照合が不一致であった場合は、エラーとなり、以下の手続きは実行されない。

#### 【0375】

個人認証が成立すると、デバイスBは、サービスプロバイダの提供するサービスに適用可能な公開鍵・秘密鍵のペアを検索（S859）する。なお、サービスプロバイダは、各ユーザとの間のデータ通信において、予め各ユーザ毎、あるいはデバイス毎に設定された公開鍵・秘密鍵のペアを用いて相互認証等、各種の暗号化処理を実行するものとする。ここでは、デバイスBの公開鍵・秘密鍵のペアが適用可能な設定である。デバイスBは、デバイスBの公開鍵証明書（PKC）を用いて、サービス登録サーバと相互認証を実行（S860）する。なお、サービス登録サーバは、管轄する1以上のサービスプロバイダ（コンテンツ配信サーバ等）のサービスを提供するユーザのユーザ登録を行なうサーバであり、各ユーザの公開鍵証明書（PKC）を登録することにより、管轄下のサービスプロバイダのサービス実行時の認証処理等、各種暗号処理を登録PKCを用いて実行可能としたサーバである。ここでは、サービス登録サーバは、各デバイスの公開鍵証明書（PKC）、または各デバイスの公開鍵証明書（PKC）と各ユーザの個人識別証明書（IDC）を登録するものとする。

#### 【0376】

サービス登録サーバとの相互認証が成立すると、次にサービス登録サーバに対するユーザAの個人認証をユーザAの個人識別証明書（IDC）を用いて実行する（S862）。これらの処理が済むと、デバイスBは、サービス登録サーバからサービス利用可能通知を受領し、利用可能なサービス情報、コンテンツ配信サーバのPKCを受信する（S864）。

#### 【0377】

以下の処理は、コンテンツ配信サーバからのコンテンツ配信を実行する処理であり、ステップS865でコンテンツ配信サーバのPKCとデバイスBのPKCとを用いて、相互認証処理を実行し、相互認証の成立を条件としてコンテンツの配信を受ける（S867）。なお、コンテンツ配信サーバは、デバイスBからのコンテンツ要求に応じて、コンテンツ要求の際の相互認証に用いられたPKCが

コンテンツ利用権のあるPKCとしてサービス登録サーバに登録されているか否かを確認する処理を実行する。確認が取れた場合にのみコンテンツの配信を行なう。サービス登録サーバには、デバイスBの公開鍵証明書（PKC）が登録済みであるので、コンテンツ要求は承認され、コンテンツが配信されることになる。

【0378】

このように、デバイスに、ユーザの個人識別証明書（IDC）、公開鍵証明書（PKC）が格納されていない場合であっても、ユーザは、個人識別認証局（IDA）に登録されたIDCをデバイスにダウンロードし、さらにデバイスに格納されたデバイスの公開鍵証明書（PKC）を用いて、IDCに基づく個人認証、PKCに基づく相互認証、データ暗号化処理を実行し、サービスプロバイダからのサービス提供を受領することが可能となる。

【0379】

#### 【12. 個人識別証明書（IDC）の有効期限設定】

これまで、説明してきたように、個人識別証明書（IDC）は個人を識別するためのテンプレート情報、例えば指紋情報、パスワード等、個人情報格納している。このテンプレート情報は暗号化されているものの、暗号解読、改竄の可能性が全くゼロであるとは言えず、管理されない個人識別証明書（IDC）が氾濫する結果を招くことは好ましいとはいえない。従って、個人識別認証局（IDA）により発行され、ユーザデバイス（UD）、あるいはサービスプロバイダ（SP）において使用される個人識別証明書（IDC）の管理が重要となる。

【0380】

ここでは、個人識別証明書（IDC）にIDC自体の有効情報として、IDCの有効期限、有効利用回数を設定し、さらに、個人識別証明書（IDC）に格納したテンプレート情報の有効期限を設定することにより、IDCおよびテンプレートが無限に使用可能な状態となることを防止するIDC管理構成について説明する。有効期限の設定により、例えば定期的なユーザ審査が可能となり、また、個人識別証明書（IDC）の発行対象者に対する有効性確認が容易となる。

【0381】

図79に、個人識別証明書（IDC）の有効情報（有効期限および有効利用回

数)と、IDCに格納したテンプレート情報の有効期限とを設定した個人識別証明書構成を示す。個人識別認証局(IDA)1001は、ユーザの個人識別証明書(IDC)を発行し、個人認証処理実行エンティティであるサービスプロバイダ(SP)1002, ユーザ端末1003に配布する。サービスプロバイダ(SP)1002, ユーザ端末1003においては、IDAから発行された個人識別証明書(IDC)を格納し、ユーザから入力されるサンプリング情報との照合処理を実行して個人認証を行なう。

#### 【0382】

個人識別認証局(IDA)1001により発行される個人識別証明書(IDC)には、図に示すように[利用有効期限または有効回数]1004、[テンプレート有効期限]1005、が格納され、全体に個人識別認証局(IDA)の秘密鍵による署名1006がなされている。署名1006は、個人識別証明書(IDC)を受領したサービスプロバイダ1002、ユーザデバイス1003において、個人識別認証局(IDA)1001の公開鍵を用いて検証され、個人識別証明書(IDC)の改竄の有無がチェックされる。

#### 【0383】

個人識別証明書(IDC)に格納された[利用有効期限または有効回数]1004は、IDC自体の有効期限を定めたデータである。これらは、個人識別証明書(IDC)の発行主体である個人識別認証局(IDA)1001により設定され、IDCに格納される。個人識別認証局(IDA)1001は、同一のユーザのテンプレート情報を格納したIDCであっても、提供先となるサービスプロバイダ、またはユーザデバイスに応じて異なる[利用有効期限、有効回数]を設定したIDCを作成して提供することができる。IDCを用いた個人認証を実行するサービスプロバイダ、またはユーザデバイスでは、サンプリング情報との照合を実行する前に個人識別証明書(IDC)に格納された[利用有効期限または有効回数]を検証し、指定期限、指定回数を満足している場合にのみ、照合処理を実行する。

#### 【0384】

個人識別証明書(IDC)に格納された[テンプレート有効期限]1005は



、IDCに格納されたテンプレート情報の有効期限を定めたデータである。これらは、個人識別証明書（IDC）の発行主体である個人識別認証局（IDA）1001により設定されるか、あるいはテンプレート情報の元データである個人データを提供したユーザ自体が設定する。ユーザがテンプレート情報の有効期限を設定する場合は、個人識別データとともに、有効期限情報を個人識別認証局（IDA）1001に送付し、個人識別認証局（IDA）1001が受領した有効期限情報に基づいてテンプレート情報の有効期限を設定してIDCに格納する。IDCを用いた個人認証を実行するサービスプロバイダ、またはユーザデバイスでは、サンプリング情報とIDC内のテンプレートとの照合を実行する前に個人識別証明書（IDC）に格納された「利用有効期限または有効回数」を検証するとともに、テンプレート情報の「テンプレート有効期限」を検証し、指定期限を満している場合にのみ、照合処理を実行する。

#### 【0385】

図80に個人識別証明書（IDC）に格納された「利用有効期限または有効回数」、およびテンプレート情報の「テンプレート有効期限」の管理構成を説明する図を示す。図80（a）は、IDCの有効期限1014と、テンプレートの有効期限1015を格納した例であり、図80（b）は、IDCの有効利用回数1017と、テンプレートの有効期限1015を格納した例である。

#### 【0386】

サービスプロバイダ、またはユーザデバイスは、図80（a）のIDCの有効期限1014と、テンプレートの有効期限1015を格納したIDCを、自己の記憶装置に格納する際は、IDCの署名1016の検証を実行してデータ改竄の無いことを確認した上で格納する。また格納したIDCを用いて個人認証を実行する場合は、ユーザの提供するサンプリング情報との比較処理ステップの前にIDCに格納されたIDCの有効期限1014と、テンプレートの有効期限1015を検証し、期限内である場合にのみ処理が続行され、期限を過ぎている場合は処理エラーとしてサンプリング情報との照合を実行しない。

#### 【0387】

サービスプロバイダ、またはユーザデバイスは、図80（b）のIDCの有効

利用回数 1 0 1 7 と、テンプレートの有効期限 1 0 1 5 を格納した IDC を、自己の記憶装置に格納する際は、IDC の署名 1 0 1 6 の検証を実行してデータ改竄の無いことを確認した上で格納する。さらに、IDC に設定された IDC 利用回数 SAM 内設定情報 1 0 1 9 を自己のデバイスの SAM (Secure Application Module) 1 0 2 0 に格納する。格納データには SAM の秘密鍵による署名 1 0 1 8 を行ないデータ改竄を防止する。格納した IDC を用いて個人認証を実行する場合は、ユーザの提供するサンプリング情報との比較処理ステップの前に IDC に格納されたテンプレートの有効期限 1 0 1 5 を検証し、さらに自己のデバイスの SAM 1 0 2 0 に格納された IDC 利用回数 SAM 内設定情報 1 0 1 9 を検証し、テンプレートの有効期限が期限内であり、かつ SAM に格納された IDC 利用回数が 0 でない場合に限り、照合処理が実行され、期限を過ぎている場合、または IDC 利用回数が 0 である場合は処理エラーとしてサンプリング情報との照合を実行しない。サンプリング情報との照合処理が実行された場合は、SAM に格納された IDC 利用回数を 1 減ずる（デクリメント）処理を実行する。

## 【 0 3 8 8 】

図 8 1 に IDC 有効期限、テンプレート有効期限の管理構成を説明する図を示す。まず、個人識別証明書（IDC）の発行主体である個人識別認証局（IDA）1 0 0 1 は、IDC 有効期限、テンプレート有効期限の設定ルールを定める。個人識別証明書（IDC）の発行を望むユーザは、個人識別認証局（IDA）1 0 0 1 に対して IDC 発行に必要な個人識別情報、個人情報を提供し、個人識別認証局（IDA）1 0 0 1 は、個人確認、データ検証を実行して、正当な IDC 発行要求であることが確認された場合に、新規に個人識別証明書（IDC）を生成する。なお、オンラインで処理を実行する際は、相互認証が行われ、通信データに対する署名付加、検証処理が実行される。なお、ユーザがテンプレートの有効期限を自ら設定することを望む場合は、自己の個人情報に加え、設定希望の有効期限を IDA に対して提示し、IDA は、その有効期限を IDC にテンプレート有効期限として設定する。

## 【 0 3 8 9 】

サービスプロバイダ 1 0 0 2 は、ユーザとの取り引きが発生した場合に、ユー

ザの個人認証を実行するため、個人識別認証局（IDA）1001に対してIDC発行要求を行なう。個人識別認証局（IDA）1001は、IDC有効期限、テンプレート有効期限を設定した個人識別証明書（IDC）をサービスプロバイダ1002に対して発行する。発行する個人識別証明書（IDC）には、個人識別認証局（IDA）1001の秘密鍵による署名がなされている。なお、サービスプロバイダ1002と個人識別認証局（IDA）1001との間の通信処理を実行する際は、相互認証が行われ、通信データに対する署名付加、検証処理が行われる。

#### 【0390】

サービスプロバイダ1002は、自己の所有する個人識別認証局（IDA）1001の公開鍵を用いて署名検証処理を実行した後、IDCをメモリに格納する。ユーザの個人認証を行なう場合は、サンプリング情報との比較処理ステップの前にIDCに格納されたIDCの有効期限と、テンプレートの有効期限を検証し、期限内である場合にのみユーザからのサンプリング情報を受領し、照合処理を実行する。なお、図の例では、個人識別証明書（IDC）のテンプレート情報は、サービスプロバイダの公開鍵により暗号化されており、サービスプロバイダの秘密鍵により復号を実行してテンプレートをIDCから取り出して照合を実行する。照合が成立した場合には、ユーザの取り引き、例えばコンテンツ提供等を行なう。

#### 【0391】

図82にIDC有効利用回数、テンプレート有効期限の管理構成を説明する図を示す。まず、個人識別証明書（IDC）の発行主体である個人識別認証局（IDA）1001は、IDC有効期限、テンプレート有効期限の設定ルールを定める。個人識別証明書（IDC）の発行を望むユーザは、個人識別認証局（IDA）1001に対してIDC発行に必要な個人情報を提供し、個人識別認証局（IDA）1001は、個人確認、データ検証を実行して、正当なIDC発行要求であることが確認された場合に、新規に個人識別証明書（IDC）を生成する。ユーザがテンプレートの有効期限を自ら設定することを望む場合は、自己の個人情報に加え、設定希望の有効期限をIDAに対して提示し、IDAは、その有効期

限をIDCにテンプレート有効期限として設定する。

【0392】

サービスプロバイダ1002は、ユーザとの取り引きが発生した場合に、ユーザの個人認証を実行するため、個人識別認証局（IDA）1001に対してIDC発行要求を行なう。個人識別認証局（IDA）1001は、IDC有効利用回数、テンプレート有効期限を設定した個人識別証明書（IDC）をサービスプロバイダ1002に対して発行する。発行する個人識別証明書（IDC）には、個人識別認証局（IDA）1001の秘密鍵による署名がなされている。

【0393】

サービスプロバイダ1002は、自己の所有する個人識別認証局（IDA）1001の公開鍵を用いて署名検証処理を実行した後、IDCをメモリに格納する。さらに、IDCに設定されたIDC利用回数を自己のデバイスのSAM（Secure Application Module）に格納する。また格納したIDCを用いて個人認証を実行する場合は、ユーザの提供するサンプリング情報との比較処理ステップの前にIDCに格納されたテンプレートの有効期限を検証し、さらに自己のデバイスのSAMに格納されたIDC利用回数を検証し、テンプレートの有効期限が期限内であり、かつSAMに格納されたIDC利用回数が0でない場合に限り、照合処理が実行され、期限を過ぎている場合、またはIDC利用回数が0である場合は処理エラーとしてサンプリング情報との照合を実行しない。サンプリング情報との照合処理が実行された場合は、SAMに格納されたIDC利用回数を1減ずる（デクリメント）処理を実行する。なお、図の例では、個人識別証明書（IDC）のテンプレート情報は、サービスプロバイダの公開鍵により暗号化されており、サービスプロバイダの秘密鍵により復号を実行してテンプレートをIDCから取り出して照合を実行する。照合が成立した場合には、ユーザの取り引き、例えばコンテンツ提供等を行なう。

【0394】

次に図83を用いて、個人識別証明書（IDC）の〔利用有効期限または有効回数〕、および〔テンプレート有効期限〕に基づいたIDC利用制御処理をまとめて説明する。

## 【0395】

サービスプロバイダ、またはユーザデバイス等においてIDCによる個人認証処理が開始される（S1001）と、ユーザはユーザ識別IDと、サンプリングデータを入力または送付する（S1002）。個人認証を実行するサービスプロバイダ、またはユーザデバイスは、ユーザIDに基づいてIDC検索を実行し、IDCの有無を判定し（S1003）、IDCが存在しない場合は、個人識別認証局（IDA）に対してIDC発行要求を出力し、IDCを取得（S1004）する。

## 【0396】

次に、個人識別証明書（IDC）の〔テンプレート有効期限〕情報を取り出してテンプレート有効期限の検証を実行（S1005）し、有効期限が有効でない場合は、個人識別認証局（IDA）に対して新たな〔テンプレート有効期限〕を設定したIDCの発行要求を出力し、IDCを取得（S1006）する。

## 【0397】

次に、個人識別証明書（IDC）の〔利用有効期限〕情報を取り出してIDC有効期限の検証を実行（S1007）し、有効期限が有効でない場合は、個人識別認証局（IDA）に対して新たな〔利用有効期限〕を設定したIDCの発行要求を出力し、IDCを取得（S1008）する。

## 【0398】

次に、個人識別証明書（IDC）に〔利用有効回数〕が設定されているか否かを判定し（S1009）、設定されている場合は、自己のデバイスのSAM内のIDC利用回数を取り出してSAM内のIDC利用回数が0になっているか否かを判定し（S1010）、0である場合は、個人識別認証局（IDA）に対して新たな〔利用有効回数〕を設定したIDCの発行要求を出力し、IDCを取得（S1011）するとともに、SAM内に新規発行されたIDCの利用有効回数を設定（S1012）する。

## 【0399】

次にIDCのテンプレートを取り出し、ユーザの提供したサンプリング情報との照合処理を実行する（S1014）。照合処理終了後、IDCに有効利用回数

が設定されている場合（S1015, Yes）は、SAM内の有効利用回数を1デクリメントし（S1016）、さらに、SAM内のIDC利用回数が0になった場合（S1017, Yes）はSAM内のIDCを消去（S1018）し、照合結果に基づく処理を実行する（S1019）。

#### 【0400】

次に、図84を用い、個人識別証明書（IDC）の利用時に、IDCの【利用有効期限】の期限切れが判明した場合のIDC更新処理について説明する。

#### 【0401】

ユーザの個人識別証明書（IDC）が個人識別認証局（IDA）1001により生成され、サービスプロバイダ1002の要求により、IDCが個人識別認証局（IDA）1001からサービスプロバイダ1002に送信され、サービスプロバイダ1002の記憶手段にIDCが格納されているとする。個人識別証明書（IDC）には、【利用有効期限】が設定されている。

#### 【0402】

サービスプロバイダ1002は、ユーザの取引における個人認証処理の実行時にIDCを取り出し、IDC内の【利用有効期限】が期限切れであったことを検出すると、個人識別認証局（IDA）1001に対して、IDCの発行依頼を実行する。この場合、更新の必要なIDCに対応するユーザIDを個人識別認証局（IDA）1001に送信する。なお、データ通信においては、相互認証、署名付加、検証処理が実行される。

#### 【0403】

個人識別認証局（IDA）1001は、ユーザIDに基づいて、すでに格納済みのユーザテンプレート情報を用いて、新たな有効期限を設定した個人識別証明書（IDC）を生成してサービスプロバイダ1002に送信する。サービスプロバイダは、更新されたIDCを自身の記憶手段に格納し、更新したIDCからテンプレートを取り出し、復号してサンプリング情報との比較照合処理を実行する。

#### 【0404】

なお、上述のIDCの有効期限の更新処理は、IDCの有効利用回数の更新、

および個人識別認証局（IDA）が設定するテンプレート有効期限の有効性消失時においても同様の手続きが適用可能である。

【0405】

図85に、定期的な個人識別証明書（IDC）の期限チェックを実行して、IDCの【利用有効期限】の期限切れが判明した場合のIDC更新処理について説明する。

【0406】

ユーザの個人識別証明書（IDC）が個人識別認証局（IDA）1001により生成され、サービスプロバイダ1002の要求により、IDCが個人識別認証局（IDA）1001からサービスプロバイダ1002に送信され、サービスプロバイダ1002の記憶手段にIDCが格納されているとする。個人識別証明書（IDC）には、【利用有効期限】が設定されている。

【0407】

サービスプロバイダ1002は、定期的に自身の格納した個人識別証明書（IDC）の有効期限のチェック処理を実行する。この定期検査時に、IDC内の【利用有効期限】が期限切れであったことを検出すると、個人識別認証局（IDA）1001に対して、IDCの発行依頼を実行する。この場合、更新の必要なIDCに対応するユーザIDを個人識別認証局（IDA）1001に送信する。なお、データ通信においては、相互認証、署名付加、検証処理が実行される。

【0408】

個人識別認証局（IDA）1001は、ユーザIDに基づいて、すでに格納済みのユーザテンプレート情報を用いて、新たな有効期限を設定した個人識別証明書（IDC）を生成してサービスプロバイダ1002に送信する。サービスプロバイダは、更新されたIDCを自身の記憶手段に格納する。

【0409】

なお、上述のIDCの有効期限の更新処理は、IDCの有効利用回数の更新、および個人識別認証局（IDA）が設定するテンプレート有効期限の有効性消失時においても同様の手続きが適用可能である。

【0410】

次に、テンプレート情報の更新処理について説明する。テンプレートの更新は、既に個人識別認証局（IDA）1001に登録済みのテンプレート情報の有効期限を単に更新する場合と、既に登録済みのテンプレート情報を削除し、新たな指紋情報等の個人情報をユーザが入力して、その新たな個人情報に基づいてテンプレート情報を再生成する場合がある。前記の登録済みのテンプレート情報を用い、有効期限を再設定する場合は、前述のIDCの有効期限、有効利用回数と同様の処理を実行すればよい。また、ユーザによってテンプレート情報の有効紀元が設定されている場合であっても、ユーザの了承を得ることで、個人識別認証局（IDA）1001において、テンプレート有効期限を再設定した個人識別証明書（IDC）を生成することが可能である。

#### 【0411】

しかし、既に登録済みのテンプレート情報を削除し、新たな指紋情報等の個人情報をユーザが入力して、その新たな個人情報に基づいてテンプレート情報を再生成する場合は、ユーザからの新たな個人識別情報の取得処理が必要となる。これらの処理について図86、図87を用いて説明する。

#### 【0412】

図86は、個人識別認証局（IDA）1001に登録済みのテンプレート情報の有効期限を個人識別認証局（IDA）1001がチェックし、有効期限切れであることをユーザに通知して更新を行なう場合の処理である。

#### 【0413】

テンプレート情報の有効期限切れの通知を受領したユーザは、新たに指紋データ等の個人識別情報を、個人識別認証局（IDA）1001に送信する。なお、この処理は、個人の確認処理を再度実行することになるので、オフラインで行なうことが好ましい。ただし、個人確認が可能であればオンラインで実行してもよい。その際には、ユーザ側のデバイスと個人識別認証局（IDA）1001間での相互認証、通信データに対する署名付加、検証処理が実行される。

#### 【0414】

個人識別認証局（IDA）1001では、個人確認が行われ、個人識別データをテンプレート情報として格納して新たなテンプレート有効期限を設定して、個



人識別証明書（IDC）を生成する。この有効期限は、ユーザ自身の設定要求に応じたデータとすることも可能である。個人識別認証局（IDA）1001によって新たにテンプレート有効期限の設定された個人識別証明書（IDC）は、要求に応じてサービスプロバイダ等に送信され、個人認証が実行される。

【0415】

図87は、ユーザ自身が自発的に個人識別認証局（IDA）1001に登録済みのテンプレート情報の更新を要求した場合の処理を説明する図である。

【0416】

テンプレート情報の更新要求を行なうユーザは、新たに指紋データ等の個人識別情報を、個人識別認証局（IDA）1001に送信する。なお、この処理は、個人の確認処理を再度実行することになるので、オフラインで行なうことが好ましい。ただし、個人確認が可能であればオンラインで実行してもよい。その際には、ユーザ側のデバイスと個人識別認証局（IDA）1001間での相互認証、通信データに対する署名付加、検証処理が実行される。

【0417】

個人識別認証局（IDA）1001では、個人確認が行われ、個人識別データをテンプレート情報として格納して新たなテンプレート有効期限を設定して、個人識別証明書（IDC）を生成する。この有効期限は、ユーザ自身の設定要求に応じたデータとすることも可能である。さらに、個人識別認証局（IDA）1001では、例えばユーザの要求等、必要に応じて、現在有効期限内にある発行済みの個人識別証明書（IDC）の無効化処理を実行する。IDCの無効化処理は、IDC失効リストを既にIDCを発行したサービスプロバイダ、ユーザデバイスに対して発行する処理として実行する。IDC失効リストには失効したIDCの識別データが記録されている。IDC失効リストを受信したサービスプロバイダ、ユーザデバイスはIDCを利用した個人認証を実行する際、IDC失効リストに使用予定のIDC識別子が記録されているか否かをチェックし、記録されている場合は、そのIDCの使用を中止する。必要であれば、新たに個人識別認証局（IDA）1001に対して更新IDCを要求して、その更新IDCを用いて個人認証を実行する。

## 【 0 4 1 8 】

上述のように、個人認証処理実行エンティティは、個人識別データであるテンプレートを格納した個人識別証明書に基づく個人認証処理の際に、証明書有効期限または証明書有効利用回数、またはテンプレート有効期限に基づき個人識別証明書の有効性確認処理を実行して、有効性が確認された場合にのみ、個人識別証明書に格納されたテンプレートと、ユーザ入力サンプリング情報との照合による個人認証を実行するので、個人識別認証局による個人識別証明書の有効性管理が可能となり、認証処理実行エンティティまたは、被認証者の要求に応じて、個人識別認証局が個人識別証明書あるいはテンプレートの更新を実行する構成としたので、任意のタイミングでの個人識別証明書あるいはテンプレートの更新処理が可能となる。上述のような有効期限の設定により、例えば定期的なユーザ審査が可能となり、また、個人識別証明書（IDC）の発行対象者に対する有効性確認が容易となる。

## 【 0 4 1 9 】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

## 【 0 4 2 0 】

## 【発明の効果】

上述したように、本発明の公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置においては、様々なデバイスにおいて容易に個人識別データであるテンプレートとユーザ入力サンプリング情報との照合による個人認証が可能となる。個人認証処理を実行する例えばサービスプロバイダ（SP）、ユーザデバイス（UD）は、第三者機関である個人識別認証局（IDA）が生成した個人識別証明書（IDC）からテンプレートを取得して個人認証を実行することが可能となる。個人識別証明書（IDC）は、個人識別認証局（IDA）がIDC発行要求者の個人確認処理を実行して、個人識別データとしてテンプレートを

取得し生成するものであり、またサービスプロバイダ（SP）、ユーザデバイス（UD）に対する配布時には、IDAの署名がなされて配布される構成であるのでデータの正当性が保証され、正確な個人認証処理が可能となる。

#### 【0421】

さらに、本発明の公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置においては、公開鍵証明書の発行要求者の個人識別データとしてのテンプレートを個人識別証明書から取得し、テンプレートとサンプリング情報との照合処理により個人認証を実行し、個人認証の成立を条件として、要求者の公開鍵証明書を発行する構成としたので、公開鍵証明書の発行手続きが簡素化され、迅速な公開鍵証明書発行処理が可能となる。

#### 【0422】

さらに、本発明の公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置においては、個人認証は個人識別認証局において実行され、公開鍵証明書を発行する認証局は、個人識別認証局の個人認証の成立を条件として公開鍵証明書を発行することが可能となるので、認証局における個人確認処理負担が軽減される。

#### 【0423】

さらに、本発明の公開鍵証明書利用システム、公開鍵証明書利用方法、および情報処理装置においては、個人識別認証局によるユーザサンプリング情報と個人識別証明書の格納テンプレートとの照合処理による個人認証成立を条件として、ユーザに対して発行される公開鍵証明書は、公開鍵証明書を受領した情報処理装置における公開鍵証明書の利用処理完了に伴い削除処理が実行されるので、個人識別認証局の個人認証に基づく公開鍵証明書特有の処理においてのみ利用可能な構成が実現される。

#### 【図面の簡単な説明】

##### 【図1】

従来の指紋読み取り照合処理を実行する個人認証装置を示す図である。

##### 【図2】

本発明の個人認証システムを利用し、かつ公開鍵証明書を用いた暗号化データ

通信の概略を説明する図である。

【図 3】

公開鍵証明書のデータ構成を説明する図である。

【図 4】

公開鍵証明書のデータ構成を説明する図である。

【図 5】

個人識別証明書のフォーマット例を示す図である。

【図 6】

個人識別証明書のテンプレートの暗号化態様を説明する図である。

【図 7】

個人識別証明書のテンプレートの暗号化に適用する鍵の種類および処理態様を説明する図である。

【図 8】

個人識別証明書のテンプレートの暗号化態様を説明する図である。

【図 9】

テンプレート登録、IDC生成処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 10】

テンプレート削除処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 11】

テンプレート変更処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 12】

テンプレート追加処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 13】

テンプレート停止処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 1 4】

テンプレート停止解除処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 1 5】

I D C 配布処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 1 6】

I D C 更新処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 1 7】

I D C 削除処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 1 8】

I D C 照会処理の流れを説明するフローおよびデータの流れを説明する図である。

【図 1 9】

公開鍵証明書（P K C）を発行する認証局（C A）と、個人識別証明書（I D C）を発行する個人識別認証局（I D A）と、証明書を利用するデバイスの構成例を示す図である。

【図 2 0】

公開鍵証明書（P K C）を発行する認証局（C A）と、個人識別証明書（I D C）を発行する個人識別認証局（I D A）と、証明書を利用するデバイスの構成例を示す図である。

【図 2 1】

ユーザデバイス、サービスプロバイダ（S P）、個人識別認証局（I D A）の各システムにおける照合処理の実行形態を説明する図である。

【図 2 2】

ユーザデバイスにおいて照合処理を実行する形態を説明する図である。

【図 2 3】

サービスプロバイダ（ＳＰ）において照合処理を実行する形態を説明する図である。

【図 2 4】

ＩＤＣとＰＫＣを格納したユーザデバイスにおける照合処理を説明する図である。

【図 2 5】

ＩＣカード等の個人端末に格納された個人識別証明書（ＩＤＣ）を共有型ユーザデバイスへ送信して照合処理を実行する構成について説明する図である。

【図 2 6】

ＩＣカード等の個人端末に格納された個人識別証明書（ＩＤＣ）を復号した後、共有型ユーザデバイスへ送信して照合処理を実行する構成について説明する図である。

【図 2 7】

ＩＣカード等の個人端末に格納された個人識別証明書（ＩＤＣ）を用いて個人端末側で照合処理を実行して、その結果のみを共有型ユーザデバイスへ送信する構成について説明する図である。

【図 2 8】

個人識別証明書（ＩＤＣ）のテンプレート情報がサービスプロバイダ（ＳＰ）の公開鍵で暗号化されている場合の処理を説明する図である。

【図 2 9】

ユーザデバイスに格納された個人識別証明書（ＩＤＣ）をサービスプロバイダ（ＳＰ）へ送信して照合処理を実行する構成について説明する図である。

【図 3 0】

ユーザデバイスに格納された個人識別証明書（ＩＤＣ）を復号した後、サービスプロバイダ（ＳＰ）へ送信して照合処理を実行する構成について説明する図である。

【図 3 1】

ユーザデバイスに格納された個人識別証明書（ＩＤＣ）を用いてユーザデバイス側で照合処理を実行して、その結果のみをサービスプロバイダ（ＳＰ）へ送信

する構成について説明する図である。

【図 3 2】

コンテンツ取り引きにおいて流通するコンテンツを含むセキュア・コンテナ (Secure Container) の構成を示す図である。

【図 3 3】

個人識別証明書 (IDC) のリスト構成を示す図である。

【図 3 4】

販売条件 (UCP) の具体的構成例を示す図である。

【図 3 5】

利用権データの構成例を示す図である。

【図 3 6】

セキュアコンテナに含まれる価格情報のデータ構成例を示す図である。

【図 3 7】

セキュアコンテナを利用したコンテンツの配信処理形態を示す図である。

【図 3 8】

使用制御情報 (UCS : Usage Control Status) の例を示す図である。

【図 3 9】

コンテンツを格納したセキュアコンテナをサービスプロバイダからユーザデバイスに配信する際の個人識別証明書 (IDC) の利用を説明する図である。

【図 4 0】

セキュアコンテナをサービスプロバイダから受領し、ユーザデバイスにおいて個人認証処理を実行して、正当なユーザにのみコンテンツ利用を可能とした処理フローを示す図である。

【図 4 1】

サービスプロバイダにおいて個人認証処理を実行して、正当なユーザにのみセキュアコンテナを配信する処理フローを示す図である。

【図 4 2】

セキュアコンテナを利用したコンテンツのユーザ間の配信処理形態を示す図である。

【図 4 3】

セキュアコンテナを利用したコンテンツのユーザ間の配信処理、ユーザの個人認証の異なる形態を示す図である。

【図 4 4】

セキュアコンテナをユーザデバイス A から受領し、ユーザデバイス B において個人認証処理を実行して、正当なユーザにのみコンテンツ利用を可能とした処理フローを示す図である。

【図 4 5】

コンテンツを配信する前に配信元において個人認証処理を実行して、正当なユーザにのみセキュアコンテナを配信する処理フローを示す図である。

【図 4 6】

ユーザデバイス間でのセキュアコンテナの転送処理を実行するユーザデバイス構成を中心としたブロック図である。

【図 4 7】

個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンク態様のそれぞれについて示す図である。

【図 4 8】

個人識別証明書（IDC）と公開鍵証明書（PKC）とのリンク態様のそれぞれについて示す図である。

【図 4 9】

リンクする公開鍵証明書（PKC）の個人識別証明書（IDC）に対する格納態様を説明する図である。

【図 5 0】

証明書の識別番号を他の証明書（IDC）に格納する構成例を示す図である。

【図 5 1】

リンク管理用データを用いた管理構成例を示す図である。

【図 5 2】

リンク管理用データを用いた管理構成例を示す図である。

【図 5 3】



個人認証を実行し、かつコンテンツ再生可能なユーザデバイスの構成を示す図である。

【図 5 4】

コンテンツダウンロード処理におけるデータの流れを説明する図である。

【図 5 5】

コンテンツダウンロード処理の流れを説明する詳細処理フロー図である。

【図 5 6】

コンテンツダウンロード処理の流れを説明する詳細処理フロー図である。

【図 5 7】

コンテンツダウンロード処理の流れを説明する詳細処理フロー図である。

【図 5 8】

ユーザ登録、ユーザ登録抹消、サービス契約処理におけるデータの流れを説明する図である。

【図 5 9】

ユーザ登録、ユーザ登録抹消、サービス契約処理を説明する詳細処理フロー図である。

【図 6 0】

ユーザ登録、ユーザ登録抹消、サービス契約処理を説明する詳細処理フロー図である。

【図 6 1】

ユーザ登録、ユーザ登録抹消、サービス契約処理を説明する詳細処理フロー図である。

【図 6 2】

デバイスに格納する個人識別証明書（IDC）の要求処理におけるデータの流れを説明する図である。

【図 6 3】

デバイスに格納する個人識別証明書（IDC）の要求処理の流れを説明する詳細処理フロー図である。

【図 6 4】

デバイスに格納する個人識別証明書（IDC）の要求処理の流れを説明する詳細処理フロー図である。

【図 6 5】

デバイスに格納する個人識別証明書（IDC）の要求処理の流れを説明する詳細処理フロー図である。

【図 6 6】

ワンタイムPKCの発行手順を説明する図である。

【図 6 7】

ワンタイムPKCの発行手順を示すフロー図である。

【図 6 8】

照合証明書の第 1 の利用形態を説明する図である。

【図 6 9】

照合証明書の利用処理フローを示す図である。

【図 7 0】

照合証明書の第 2 の利用形態を説明する図である。

【図 7 1】

照合証明書のフォーマット例を示す図である。

【図 7 2】

個人識別認証局（IDA）に登録済みの個人識別証明書（IDC）を利用して個人認証を行ない、さらに、個人認証処理に基づいてコンテンツ配信を受ける処理を説明する図である。

【図 7 3】

IDCを利用した個人認証、PKCを利用した相互認証を実行してコンテンツの配信サービスを実行する処理を示すフロー図である。

【図 7 4】

IDCを利用した個人認証、PKCを利用した相互認証を実行してコンテンツの配信サービスを実行する処理を示すフロー図である。

【図 7 5】

IDCを利用した個人認証、PKCを利用した相互認証を実行してコンテンツ

の配信サービスを実行する処理を示すフロー図である。

【図76】

ユーザIDCと、デバイスPKCを用い、個人識別認証局（IDA）に登録済みのIDCを利用して個人認証を行ない、デバイスPKCに基づいてコンテンツ配信を受ける処理を説明する図である。

【図77】

ユーザIDCと、デバイスPKCを用い、個人識別認証局（IDA）に登録済みのIDCを利用して個人認証を行ない、デバイスPKCに基づいてコンテンツ配信を受ける処理フローを示す図である。

【図78】

ユーザIDCと、デバイスPKCを用い、個人識別認証局（IDA）に登録済みのIDCを利用して個人認証を行ない、デバイスPKCに基づいてコンテンツ配信を受ける処理フローを示す図である。

【図79】

個人識別証明書（IDC）の有効情報（有効期限および有効利用回数）と、IDCに格納したテンプレート情報の有効期限とを設定した個人識別証明書構成を示す図である。

【図80】

個人識別証明書（IDC）に格納された「利用有効期限または有効回数」、およびテンプレート情報の「テンプレート有効期限」の管理構成を説明する図である。

【図81】

IDC有効期限、テンプレート有効期限の管理構成を説明する図である。

【図82】

IDC有効利用回数、テンプレート有効期限の管理構成を説明する図である。

【図83】

個人識別証明書（IDC）の「利用有効期限または有効回数」、および「テンプレート有効期限」に基づいたIDC利用制御処理を説明するフロー図である。

【図84】

個人識別証明書（IDC）の利用時に、IDCの〔利用有効期限〕の期限切れが判明した場合のIDC更新処理を説明する図である。

【図 8 5】

定期的な個人識別証明書（IDC）の期限チェックを実行して、IDCの〔利用有効期限〕の期限切れが判明した場合のIDC更新処理について説明する図である。

【図 8 6】

個人識別認証局（IDA）に登録済みのテンプレート情報の有効期限をIDAがチェックし、有効期限切れであることをユーザに通知して更新を行なう場合の処理を説明する図である。

【図 8 7】

ユーザ自身が自発的に個人識別認証局（IDA）に登録済みのテンプレート情報の更新を要求した場合の処理を説明する図である。

【符号の説明】

- 1 0 個人認証装置
- 1 1 個人情報取得部
- 1 2 情報変換部
- 1 3 比較部
- 1 4 セキュアメモリ
- 1 5 制御部
- 1 6 通信部
- 2 0 パーソナルコンピュータ
- 2 0 1 個人識別認証局（IDA）
- 2 0 2 認証局（CA）
- 2 0 3, 2 0 4 サービスプロバイダ（SP）
- 2 0 5, 2 0 6 ユーザデバイス
- 3 0 0 サービスプロバイダ（SP）
- 3 1 0 サンプリング情報処理部
- 3 1 1 制御部

- 3 1 2 通信部
- 3 1 3 情報変換部
- 3 1 4 個人情報取得部
- 3 1 5 公開鍵証明書
- 3 2 0 個人識別認証局 ( I D A )
- 3 2 1 比較部
- 3 2 2 記憶手段
- 3 3 0 認証局 ( C A )
- 4 0 0 サービスプロバイダ ( S P )
- 4 1 0 照合システム
- 4 1 1 通信部
- 4 1 2 制御部
- 4 1 3 メモリ
- 4 1 4 個人識別証明書検証部
- 4 1 5 テンプレート復号化部
- 4 1 6 比較部
- 4 1 7 情報変換部
- 4 1 8 個人情報取得部
- 4 1 9 暗号処理部
- 4 2 0 個人識別認証局
- 4 2 1 個人識別証明書発行部
- 4 2 2 記憶手段
- 4 3 0 認証局
- 4 5 0 I C カード
- 5 0 0 ユーザデバイス
- 5 0 1 コンテンツ再生機構部
- 5 0 2 コンテンツデータ蓄積部
- 5 0 3 個人識別装置
- 5 0 4 ネットワーク接続部

505 公開鍵暗号処理部  
506 選択機能部  
507 入出力機能部  
700 セキュアコンテナ  
701 コンテンツ  
702 価格情報  
703 販売情報 (UCP)  
704 電子署名  
711 IDC識別子リスト  
712 UCP世代管理情報  
713 二次配信可能回数  
721 IDC識別子リスト  
731 IDC識別子リスト  
732 UCS世代管理情報  
733 UCS二次配信可能回数  
801 コンテンツプロバイダ  
802 サービスプロバイダ  
803, 805 ユーザデバイス  
804 クリアリングセンタ  
810 ユーザデバイス  
820 ユーザ  
830 個人識別認証局 (IDA)  
840 サービスプロバイダ  
910 個人識別認証局 (IDA)  
920 ユーザデバイス1  
930 ユーザデバイス2  
940, 945 ユーザ  
950 ユーザデバイス1  
955, 965 個人識別証明書

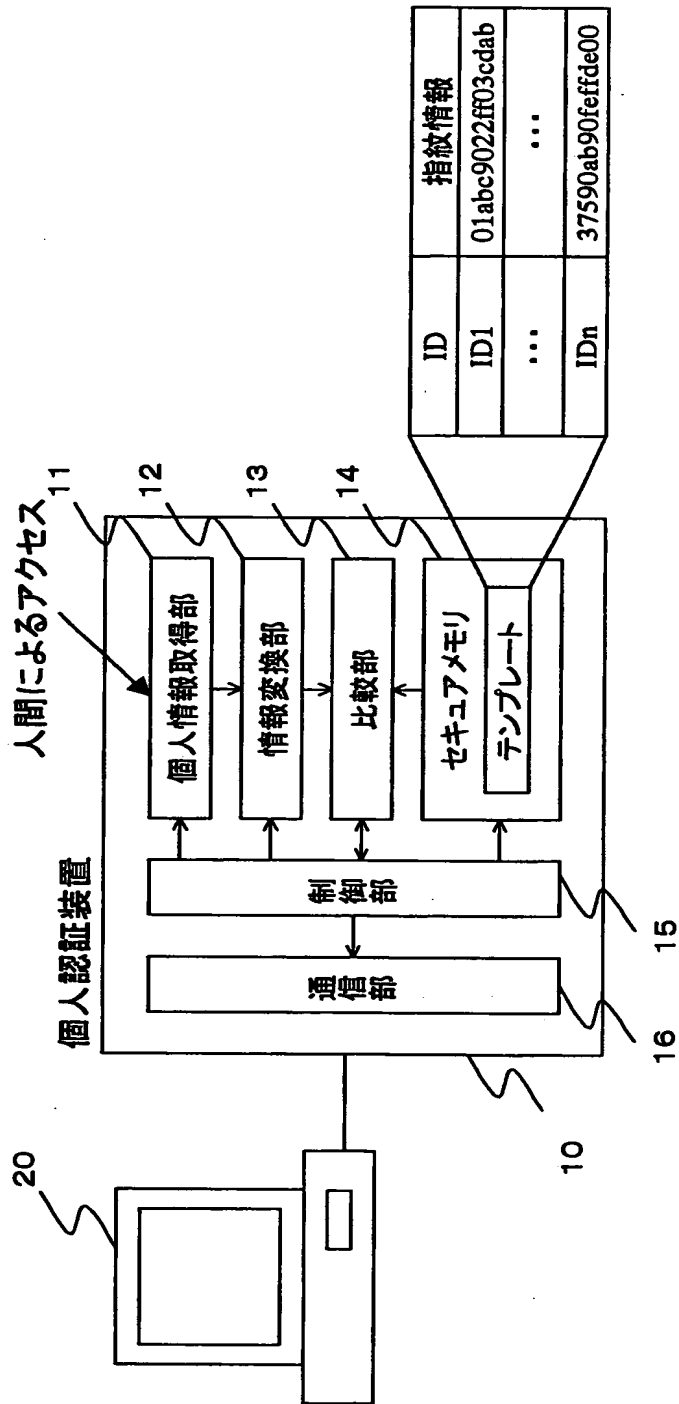
- 9 6 0 ユーザデバイス 2
- 9 7 0 個人識別認証局 ( I D A )
- 9 9 0 セキュアコンテナ
- 9 9 2 I D C 識別子リスト
- 1 0 0 1 個人識別認証局 ( I D A )
- 1 0 0 2 サービスプロバイダ
- 1 0 0 3 ユーザ端末
- 1 0 0 4 I D C 利用有効期限 / 有効回数情報
- 1 0 0 5 テンプレート有効期限情報
- 1 0 0 6 I D A 署名
- 1 0 1 4 I D C 利用有効期限
- 1 0 1 5 テンプレート有効期限情報
- 1 0 1 6 I D A 署名
- 1 0 1 7 I D C 利用有効回数
- 1 0 1 8 S A M 署名
- 1 0 1 9 I D C 利用回数 S A M 内設定情報
- 1 0 2 0 S A M ( Secure Application Module )
- 1 8 1 0 サービスプロバイダ
- 1 8 1 1 制御部
- 1 8 1 2 コンテンツデータベース
- 1 8 1 3 ユーザ情報データベース
- 1 8 1 4 暗号処理部
- 1 8 1 5 通信部
- 1 8 1 6 個人識別装置
- 1 8 2 0 ユーザデバイス A
- 1 8 3 0 ユーザデバイス B
- 1 8 2 1 , 1 8 3 1 制御部
- 1 8 2 2 , 1 8 3 2 暗号処理部
- 1 8 2 4 , 1 8 3 4 メモリ

1825, 1835 記憶部  
1826, 1836 データ再生部  
1827, 1837 通信部  
1828, 1838 電子マネー  
1829, 1839 個人識別装置  
1840 クリアリングセンタ  
1841 制御部  
1842 データベース  
1844 暗号処理部  
1845 通信部  
1846 個人識別装置

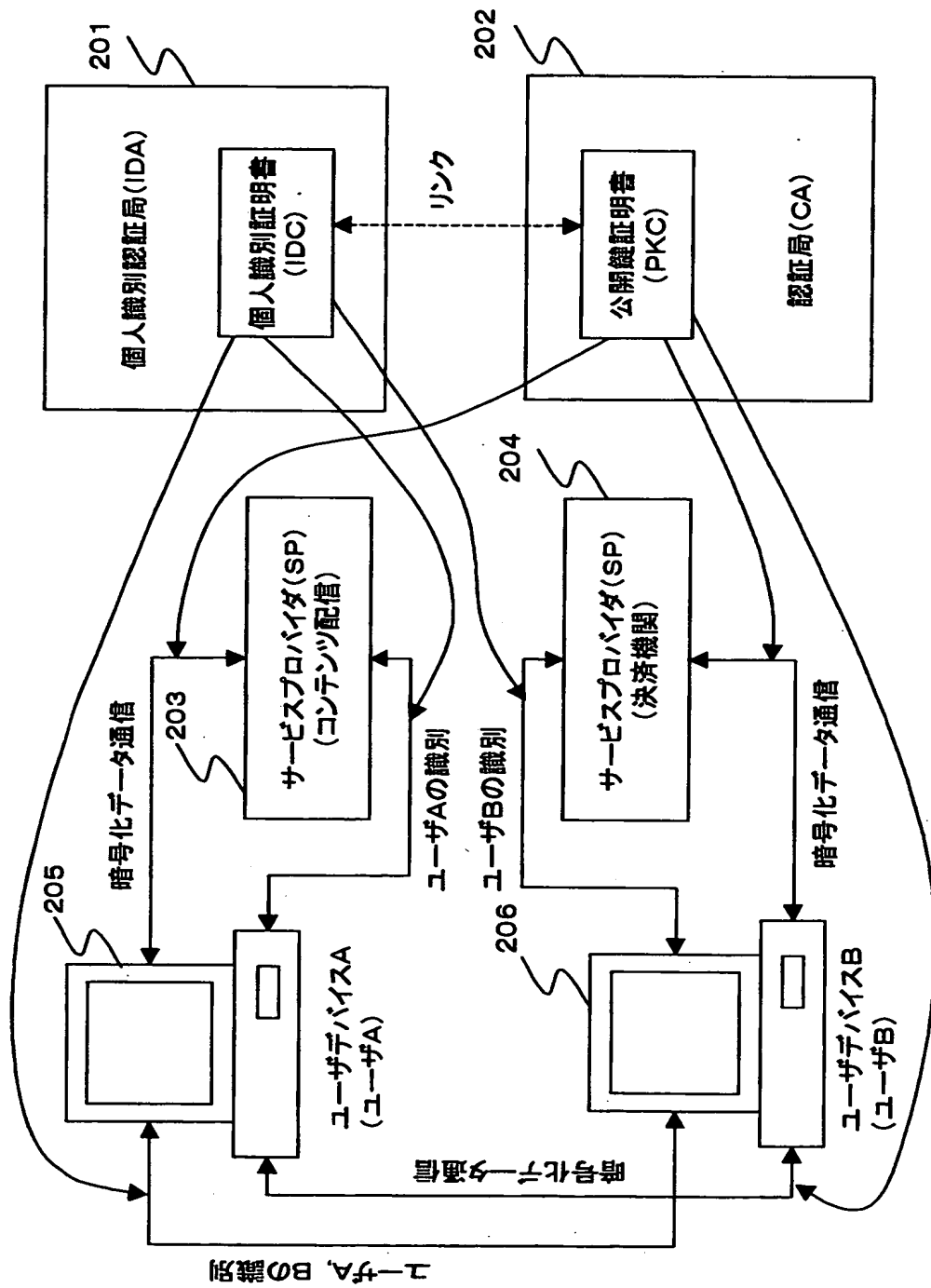


【書類名】 図面

【図 1】



【図 2】



【図 3】

| 証明書フォーマット例 (X.509 V3に準拠)   |   |  |
|--|---|--|
| 項目   | 説明  | 本IAにおける設定                                |
| Version1   |   |  |
| version  | 証明書のフォーマットのバージョン  | V3                                       |
| serial Number  | IA によってつけられる証明書のSerial No.  | シーケンシャルなシリアルナンバー                         |
| signature.algorithm Identifier<br>algorithm<br>parameters  | 証明書の署名アルゴリズム、及びそのパラメータ  | 楕円曲線暗号/RSA<br>楕円の場合パラメータ<br>RSAの場合鍵長     |
| issuer   | IA 名 (Distinguished Name形式)   | 本IAの名称                                   |
| validity<br>notBefore<br>notAfter  | 証明書の有効期限<br>開始日時<br>終了日時  |  |
| subject  | user を識別する名前  | ユーザ機器ID またはサービス主体のID                     |
| subject Public Key Info<br>algorithm<br>subject Public key   | user の公開鍵情報<br>鍵のアルゴリズム<br>鍵  | 楕円曲線RSA<br>user の公開鍵                     |
| Version3   |   |  |
| authority Key Identifier<br>key Identifier<br>authority Cert Issuer<br>authority Cert Serial<br>Number   | IA の署名確認用の鍵識別<br>鍵識別番号 (8 進数)<br>IA 名 (General Name形式)<br>認証番号  |  |
| subject key Identifier   | 複数の鍵の証明をする場合  | 利用しない                                    |
| key usage<br>(0)digital Signature<br>(1)non Repudiation<br>(2)key Encipherment<br>(3)data Encipherment<br>(4)key Agreement<br>(5)key CertSign<br>(6)cRL Sign | 鍵の使用目的を指定<br>(0)デジタル署名用<br>(1)否認防止用<br>(2)鍵の暗号化用<br>(3)メッセージの暗号化用<br>(4)共通鍵配送用<br>(5)認証の署名確認用<br>(6)失効リストの署名確認用 | 0,1,4,6を利用                               |
| private Key Usage Period<br>notBefore<br>notAfter  | user に格納されている秘密鍵の有効期限。  | 証明書の有効期限 = 公開鍵の有効期限 = 秘密鍵の有効期限 (default) |

【図 4】

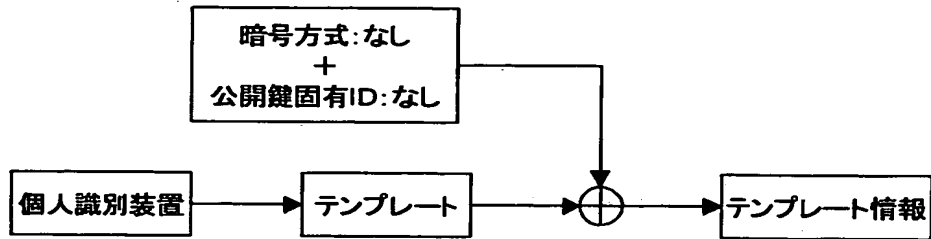
|   |  |                                 |
|---|--|---------------------------------|
| Certificate Policy<br>policy Identifier<br>policy Qualifiers                                    | 認証局の証明書発行ポリシー<br>ポリシーID(ISO/IEC9834-1に準拠)<br>認証基準                                |                                 |
| policy Mappings<br>issuer Domain Policy<br>subject Domain Policy                                | CA を認証する場合にのみ必要。発行認証局のポリシーと被認証ポリシーのマッピングを規定                                      | default = なし                    |
| supported Algorithms<br>algorithm Identifier<br>intended Usage<br>intended Certificate Policies | ディレクトリ (X.500) のアトリビュートを定義。コミュニケーションの相手がディレクトリ情報を利用する場合に、事前にそのアトリビュートを知らせるのに用いる。 | default = なし                    |
| subject Alt Name  | user の別名 (GN 形式)。  | 利用しない                           |
| issuer Alt Name   | 項目は入れておく(default = なし)   | default = なし                    |
| subject Directory Attributes  | user の任意の属性。   | 利用しない                           |
| basic Constraints   | 証明対象の公開鍵が認証  |                                 |
| ca<br>path Len Constraint   | 局の署名用か、user のものかを区別  | default = user 用                |
| name Constraints<br>permitted Subtrees<br>base<br>minimum<br>maximum<br>excluded Subtrees       | 被認証者が認証局である場合 (CA 認証) にのみ使用。   | default = なし                    |
| policy Constraints<br>requireExplicitPolicy<br>inhibitPolicyMapping                             | 認証パスの残りに対する明確な認証ポリシー ID、禁止ポリシーマップを要求する制限を記述                                      |                                 |
| CRL Distribution Points   | user が証明書を利用する際に、証明書が失効していないかどうかを確認するための失効リストの参照ポイントを記述。                         | 証明書を登録したところへのポイント。失効リストは、発行元で管理 |
| 署名  | 発行者の署名   |                                 |

【図 5】

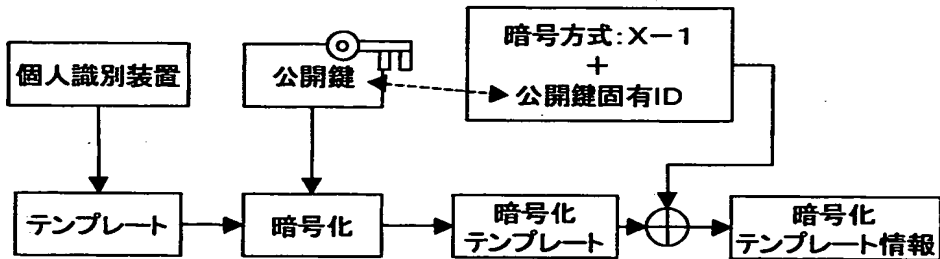
|      | 項目  | 説明  |
|------|---|---|
| 必須項目 | Version   | バージョン   |
|      | SerialNumber  | 識別番号  |
|      | signaturealgorithmIdentifier<br>algorithm<br>parameters   | 署名方式<br>アルゴリズム<br>パラメータ   |
|      | Issuer  | 個人識別認証局名(Distinguished Name形式)  |
|      | Validity<br>notBefore<br>notAfter   | 有効期限<br>・ 開始日時<br>・ 終了日時  |
|      | Subject   | 被認証者名(DN形式)   |
|      | subjectTemplateInfo<br>encryptType<br>encryptUniqueID<br>encryption Algorithm<br>parameter<br>validity<br>subjectTemplate Source<br>subjectTemplate | テンプレート情報<br>・ 暗号方式<br>・ 暗号化するために使用した公開鍵証明書の固有IDまたは認証番号<br>・ アルゴリズム<br>・ パラメータ<br>・ 有効期限 (開始日時: 終了日時)<br>・ テンプレートの種別<br>・ テンプレート |
| 拡張項目 | SubjectPKCinfo<br>subjectPKCserialNumber<br>subjectPKCUniqueID  | 被認証者の公開鍵証明書情報<br>・ 被認証者の公開鍵証明書の認証番号<br>・ 被認証者の公開鍵証明書の被認証者固有ID   |
|      | IssuerUniqueID  | 個人識別認証局の固有ID  |
|      | SubjectUniqueID   | 被認証者の固有ID   |
|      | PublicKey Certificate   | 公開鍵証明書  |
|      | Issuer Alt Name   | 個人識別認証局の別名  |
|      | subjectDirectoryAttributes  | 個人情報 (必要に応じて暗号化)<br>本人確認のための情報<br>年齢、性別、e t c   |
|      | Valid Count   | 有効回数  |
|      | Control Table Link Info<br>Ctl Tbl Location<br>Ctl Tbl Unique ID  | 組情報へのリンク情報<br>・ 組情報管理テーブルのある場所 (URL, IP address等)<br>・ 組情報識別番号  |
| 必須   | IDASignature  | IDAの署名  |

【図 6】

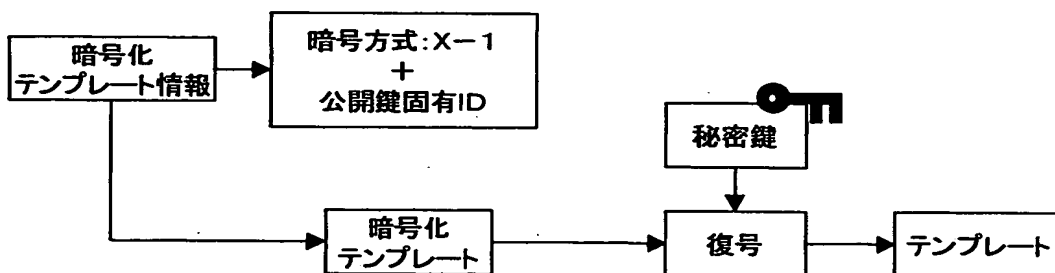
(a) 非暗号化



(b-1) 公開鍵のみを使用した暗号化



(b-2) 秘密鍵のみを使用した復号化

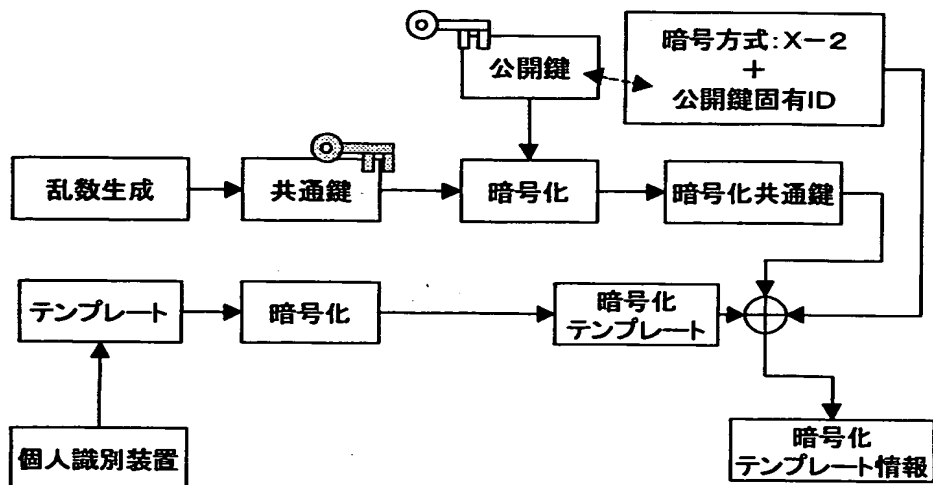


【図 7】

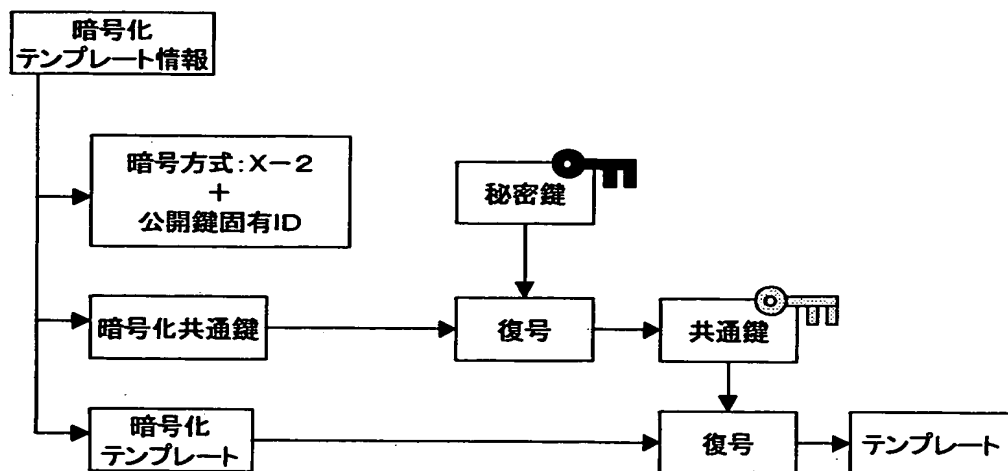
| テンプレート暗号化に<br>用いる公開鍵      | テンプレート情報格納IDCの使用例  |
|---------------------------|--|
| ユーザまたは<br>ユーザデバイスの<br>公開鍵 | ユーザデバイス(例えばPC)の使用許可を付与した<br>特定ユーザの識別を、各ユーザ毎の個人識別証明書<br>(IDC)を用いて識別処理を行なう場合等          |
| サービスプロバイダの<br>公開鍵         | サービスプロバイダにおいて、特定ユーザ、例えば<br>サービスを提供するユーザを識別するために、各ユーザの<br>個人識別証明書(IDC)を用いて個人識別を行なう場合等 |
| 個人識別認証局の<br>公開鍵           | 様々な端末間でのデータ送受信における、データ送受信者<br>において、個人識別認証局(IDA)発行の個人識別<br>証明書(IDC)を用いて個人識別処理を行なう場合等、 |

【図 8】

(c-1) 共通鍵と公開鍵を使用した暗号化

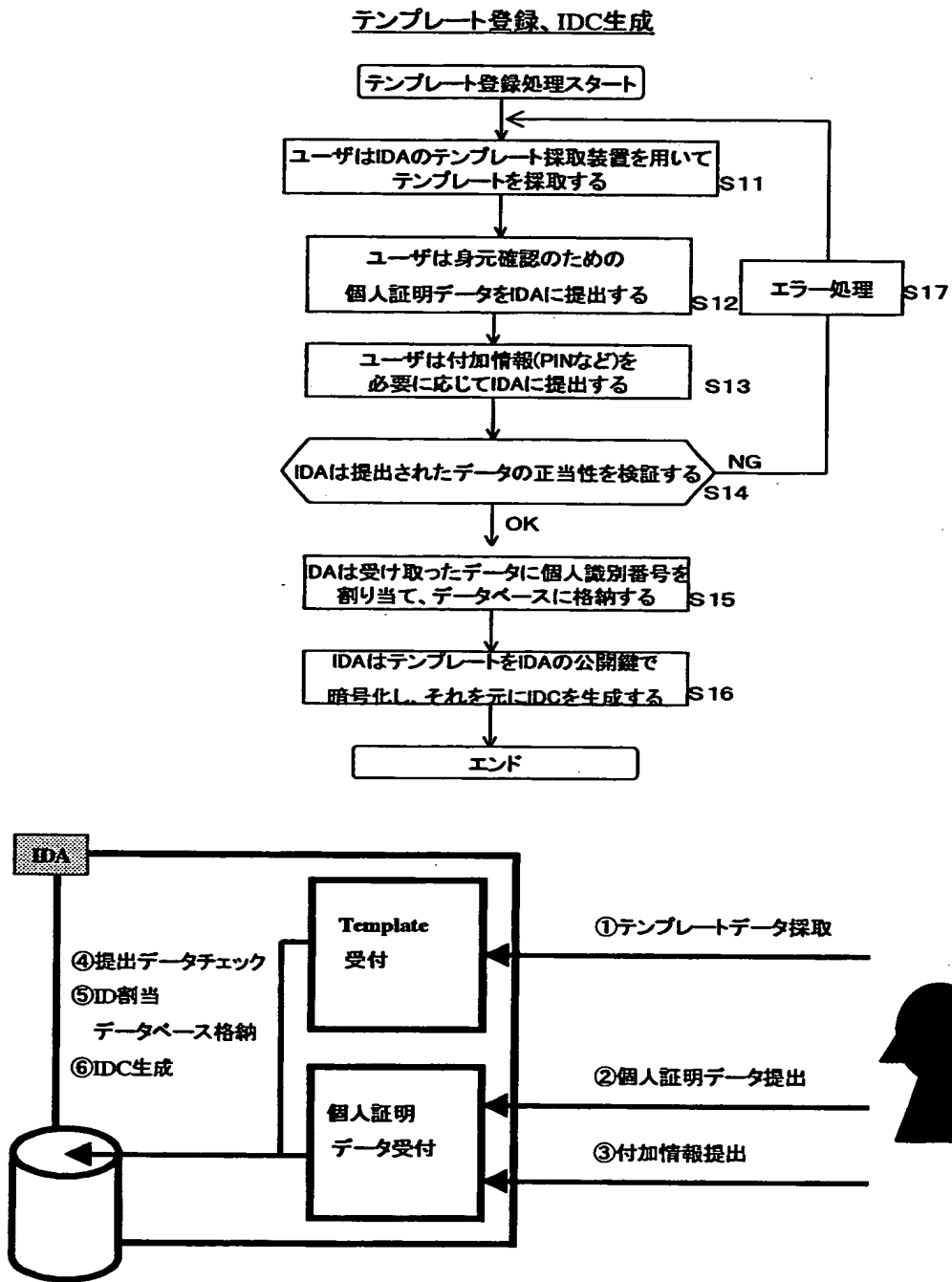


(c-2) 共通鍵と秘密鍵を使用した復号化

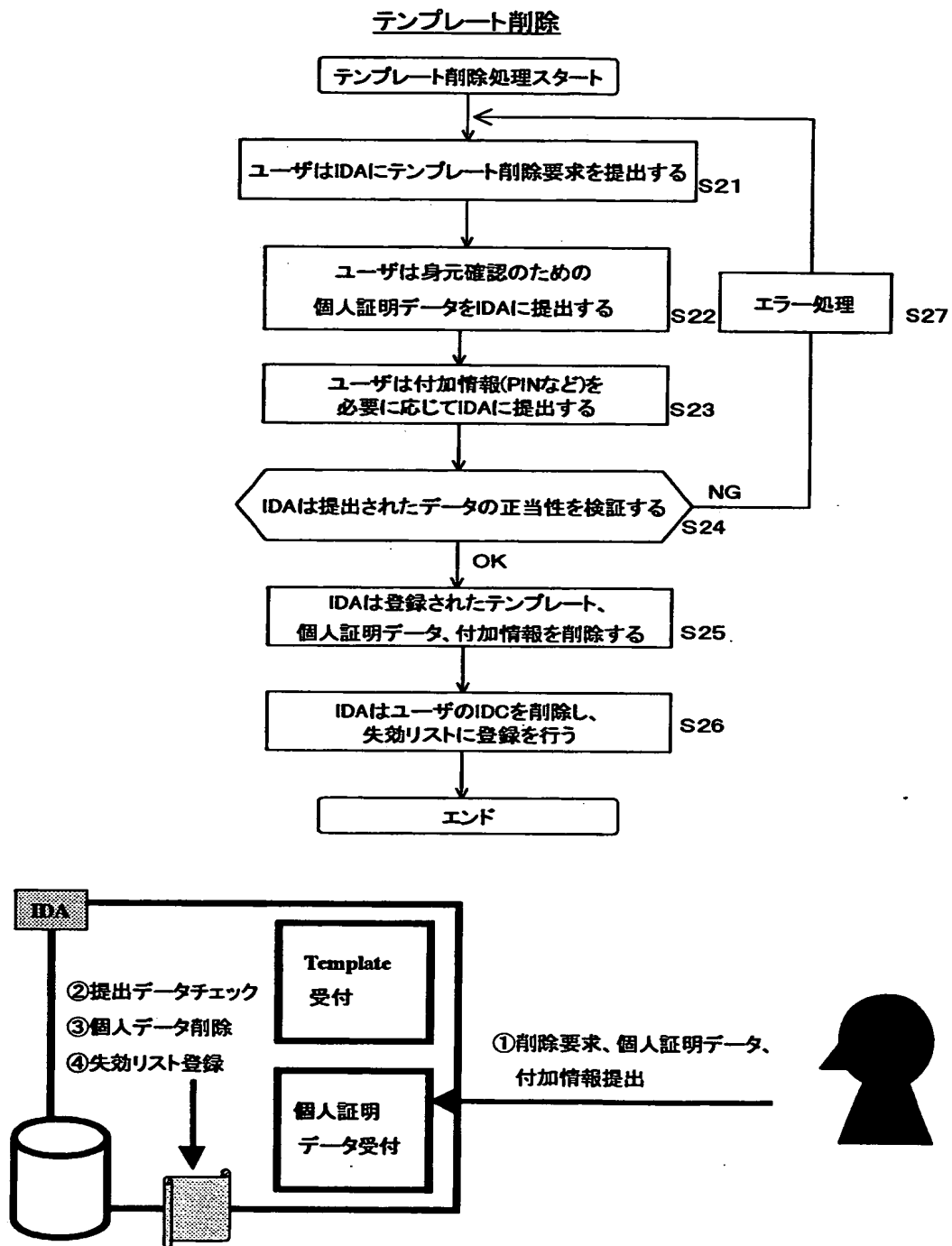




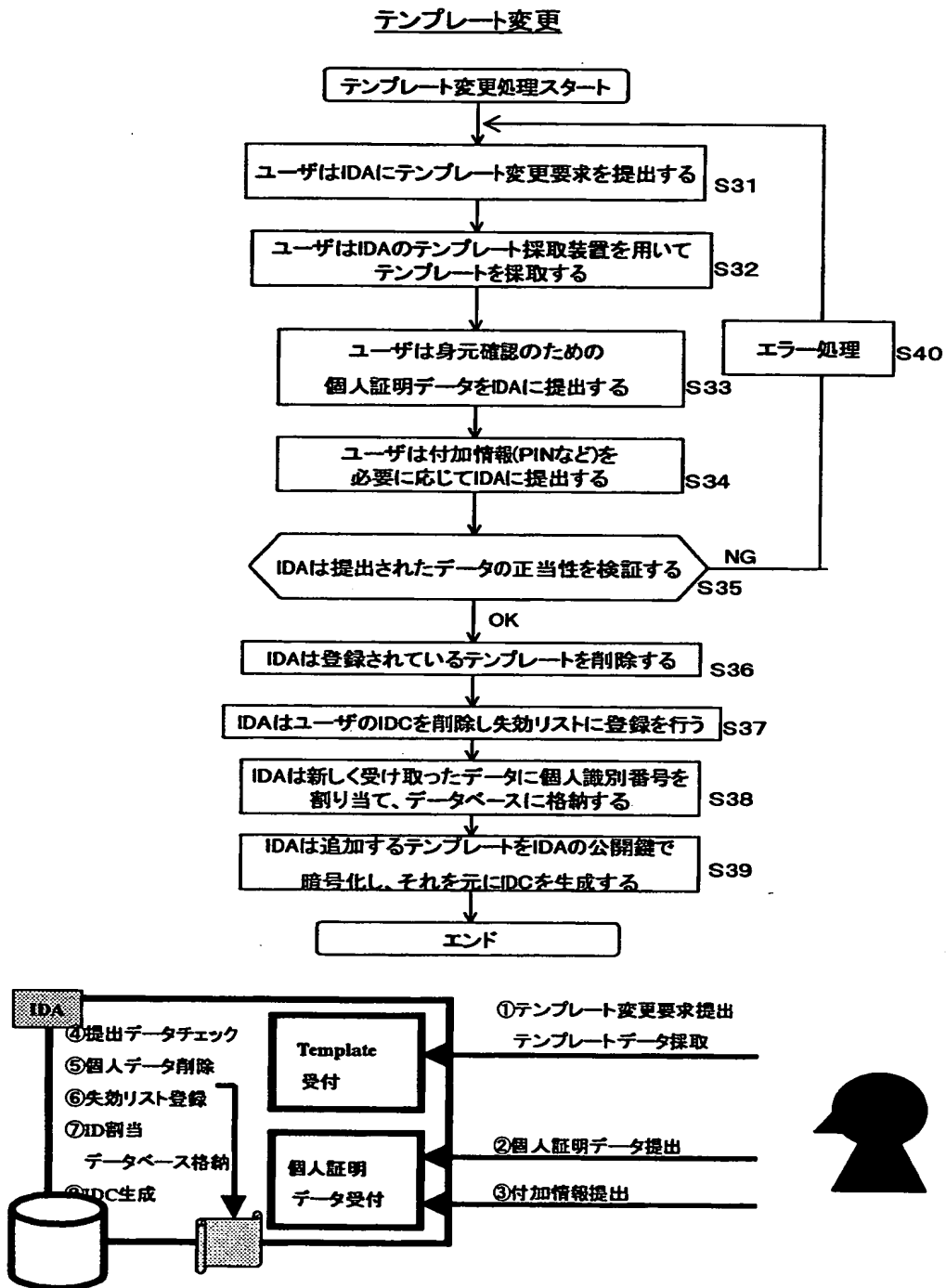
【図 9】



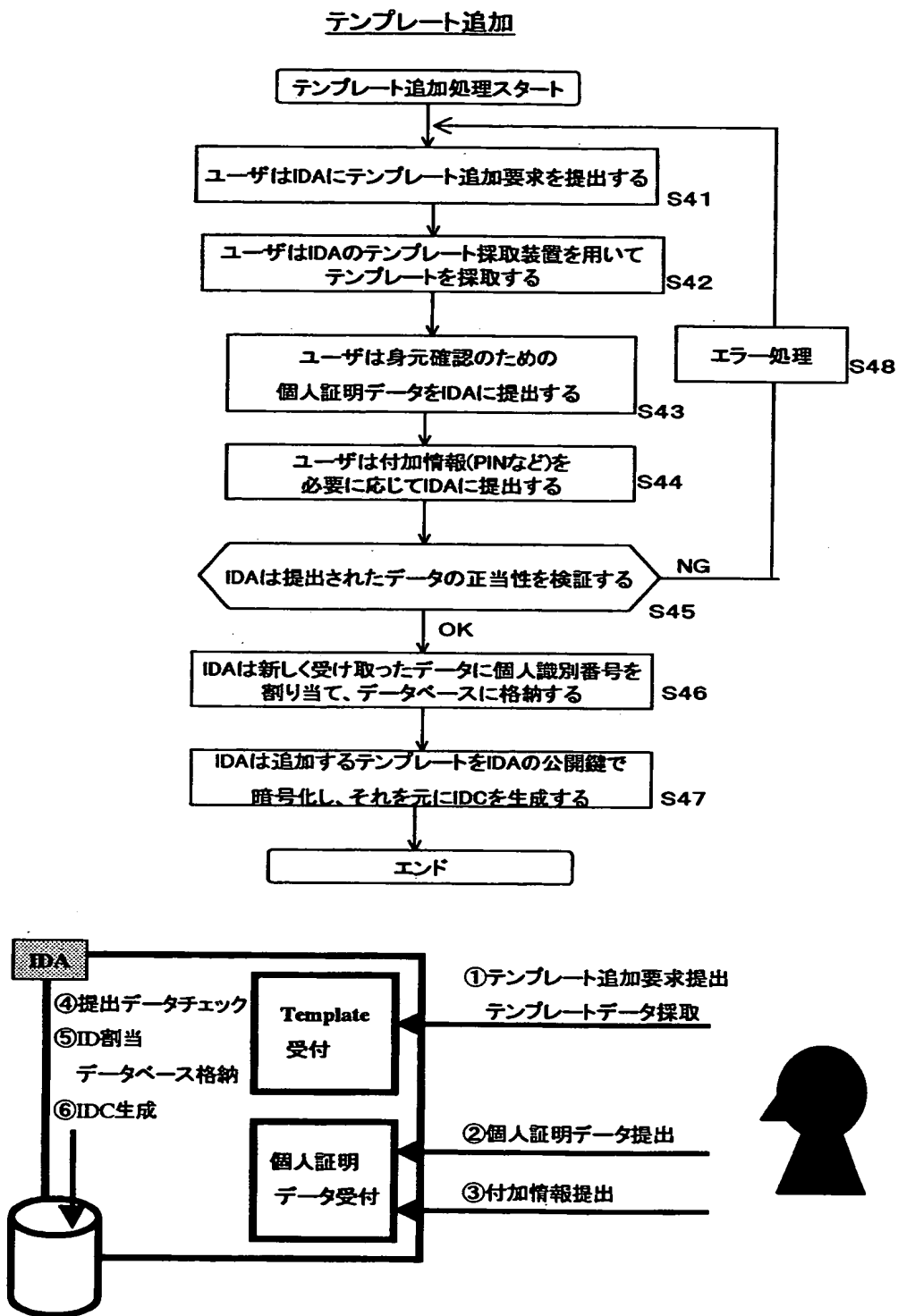
【図 1 0】



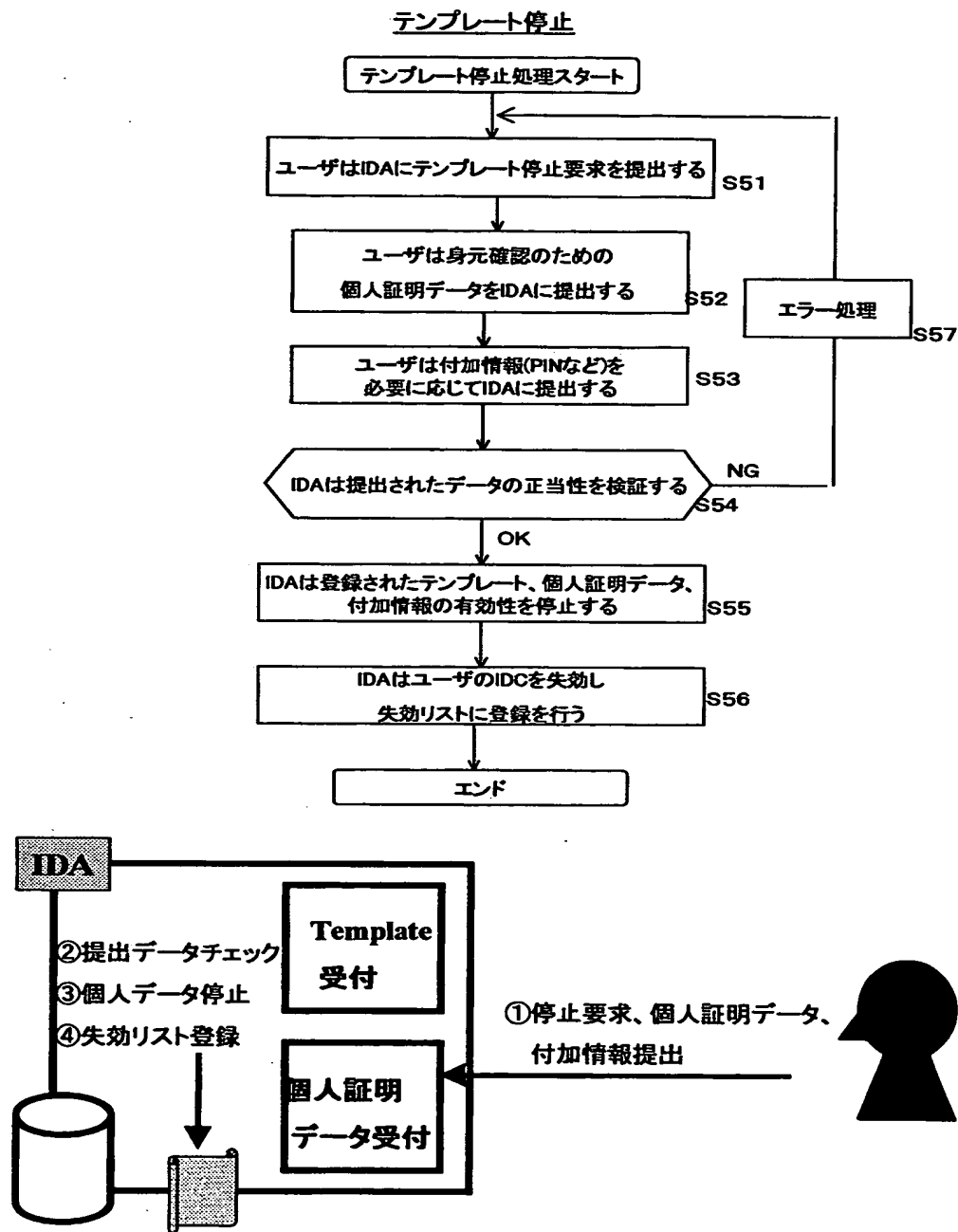
【図 11】



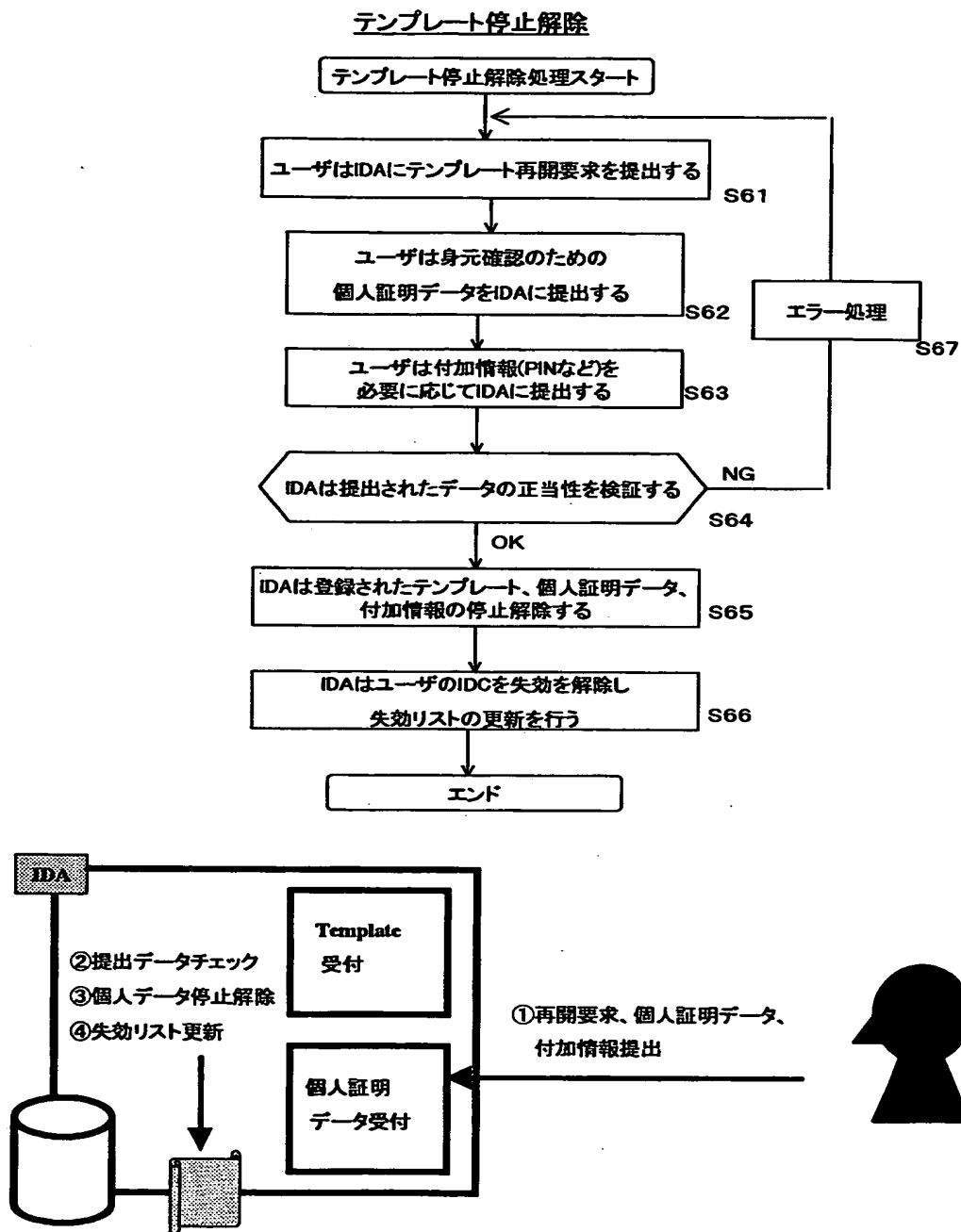
【図 12】



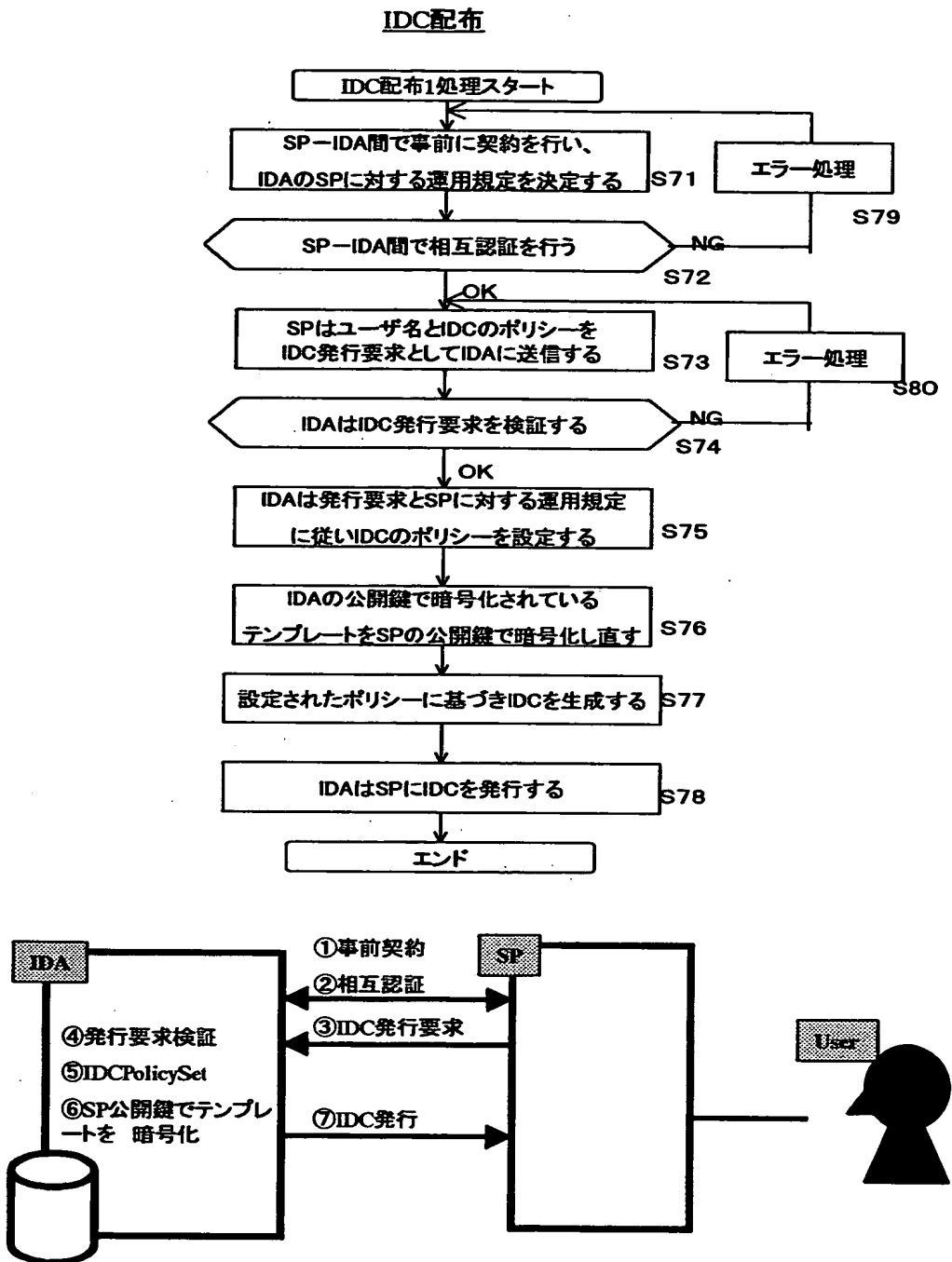
【図 13】



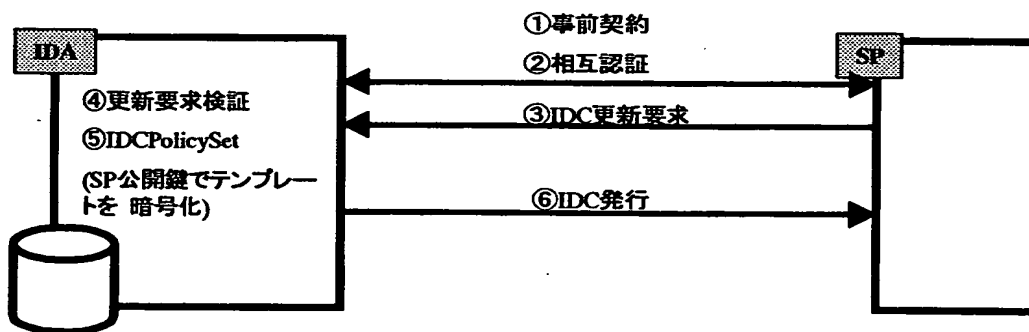
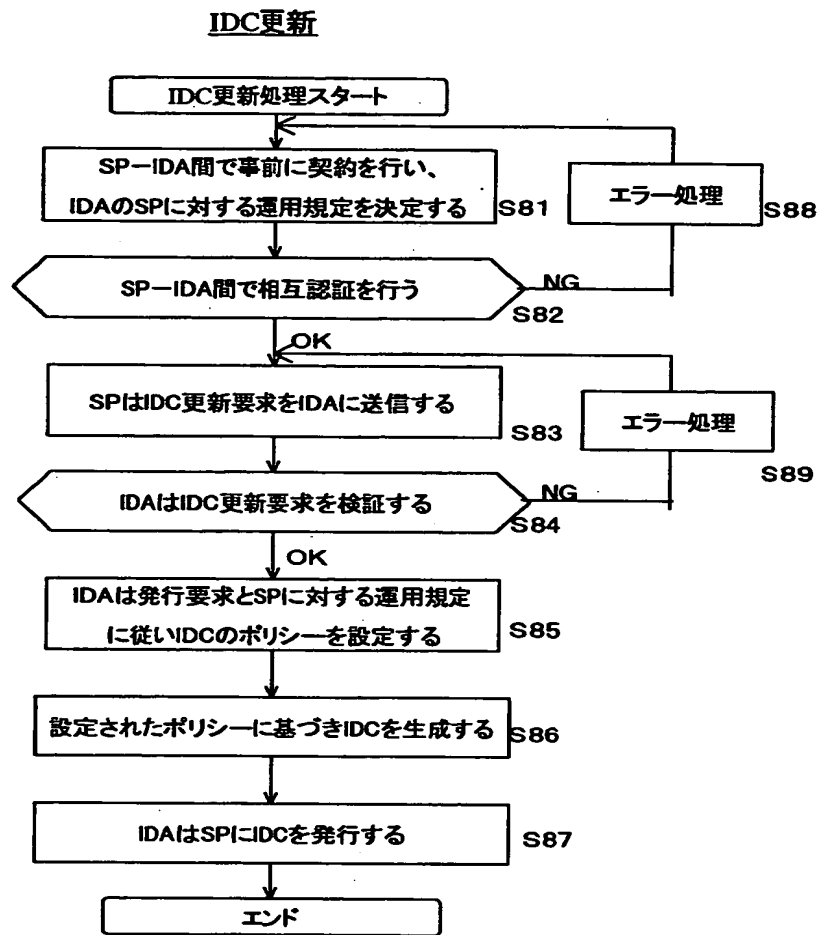
【図 14】



【図 15】



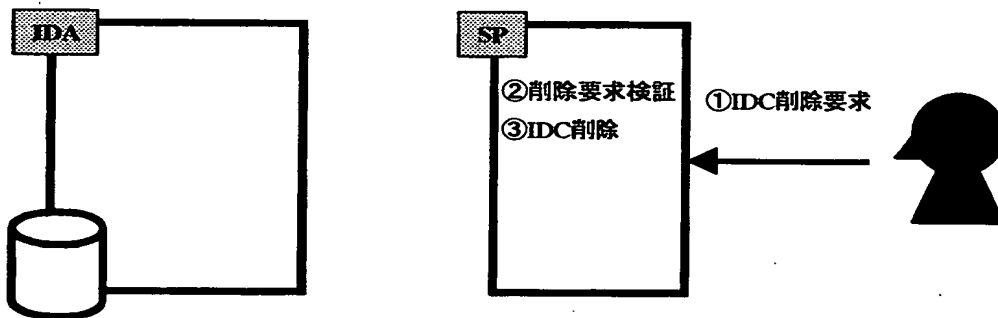
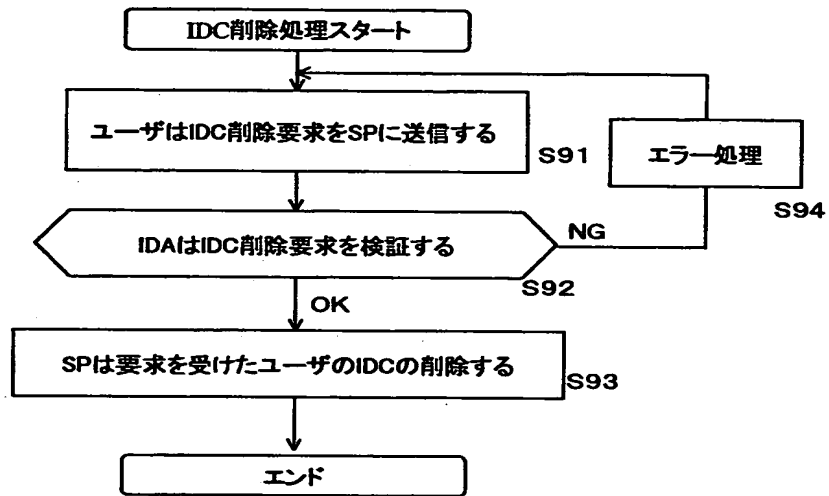
【図 16】



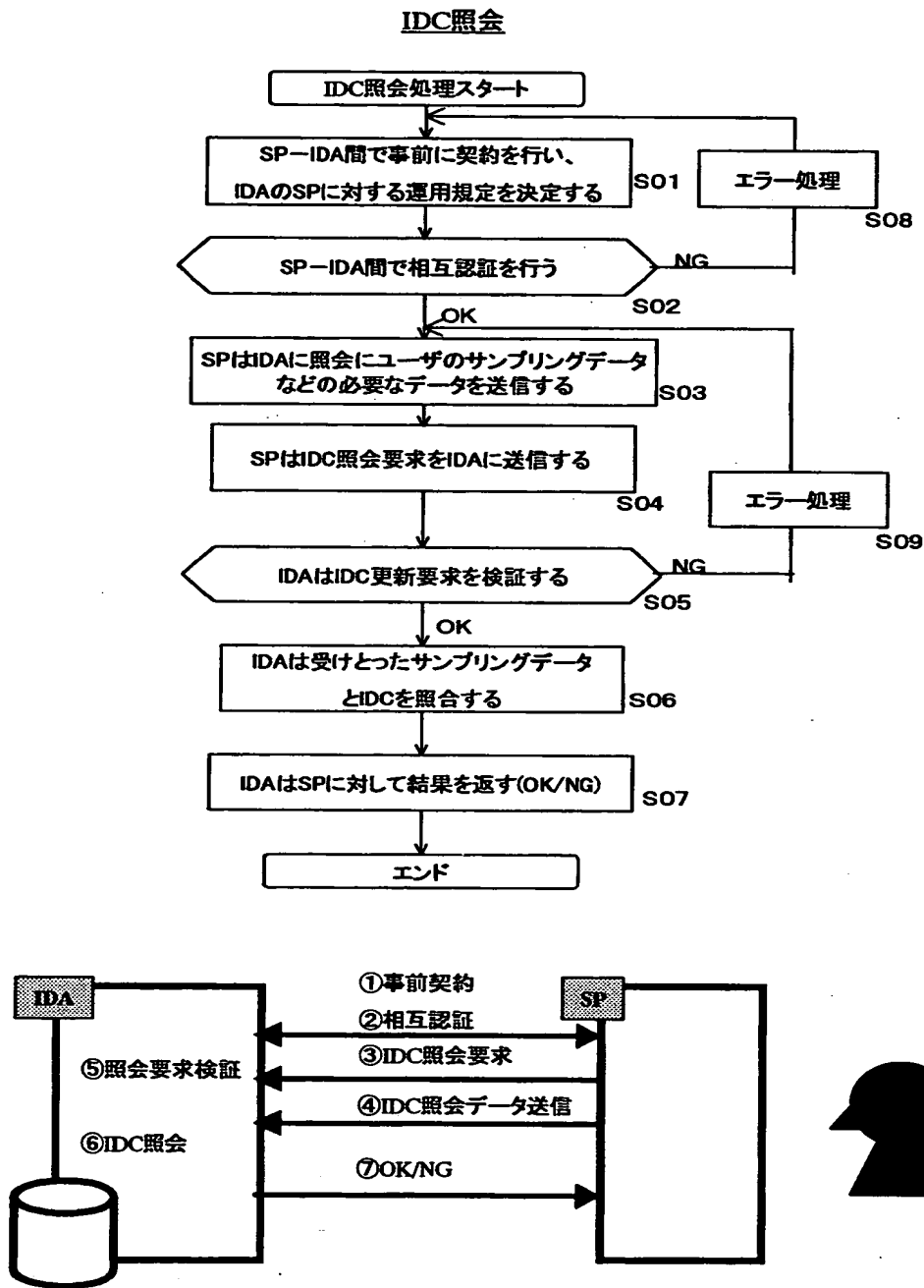


【図 1 7】

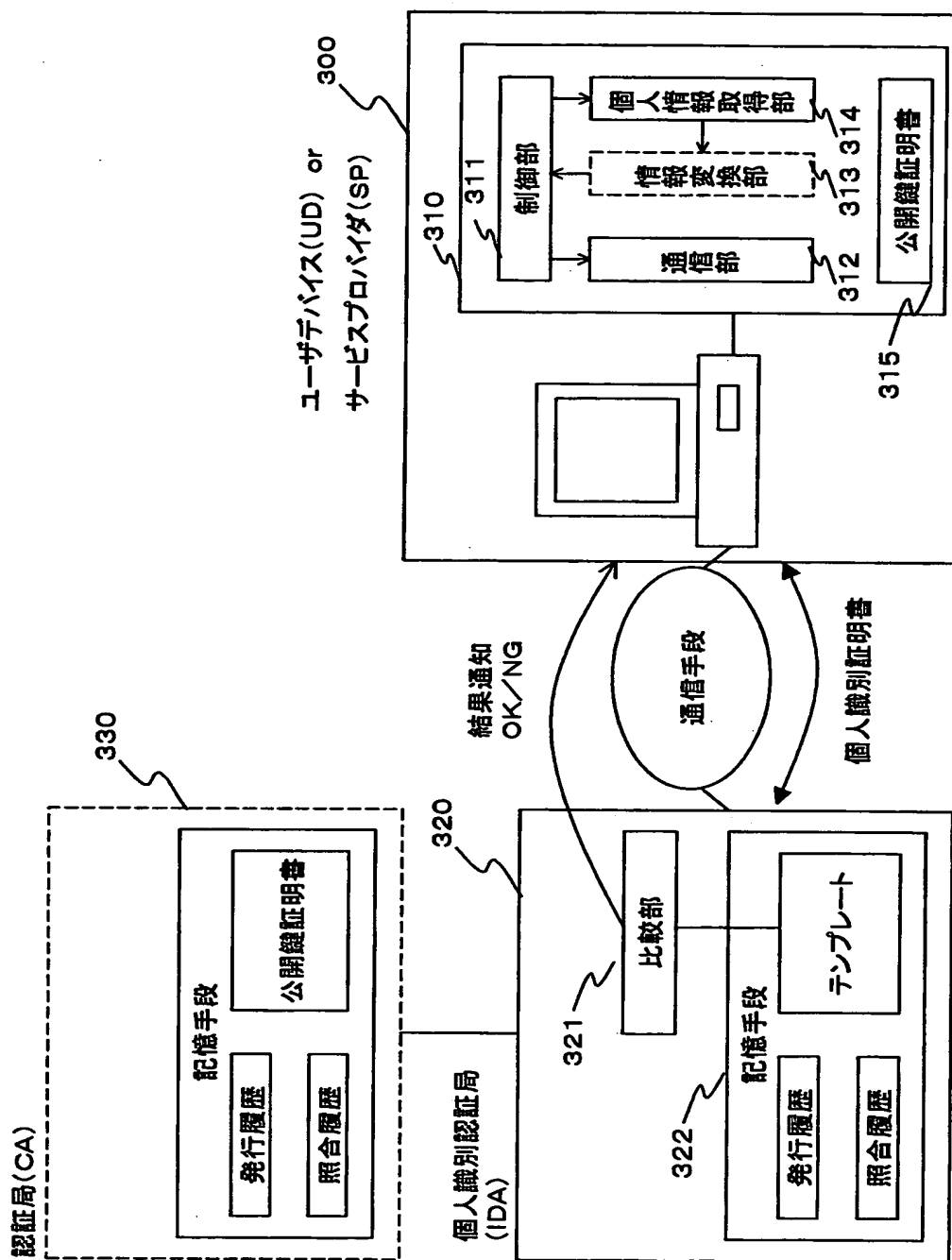
IDC削除



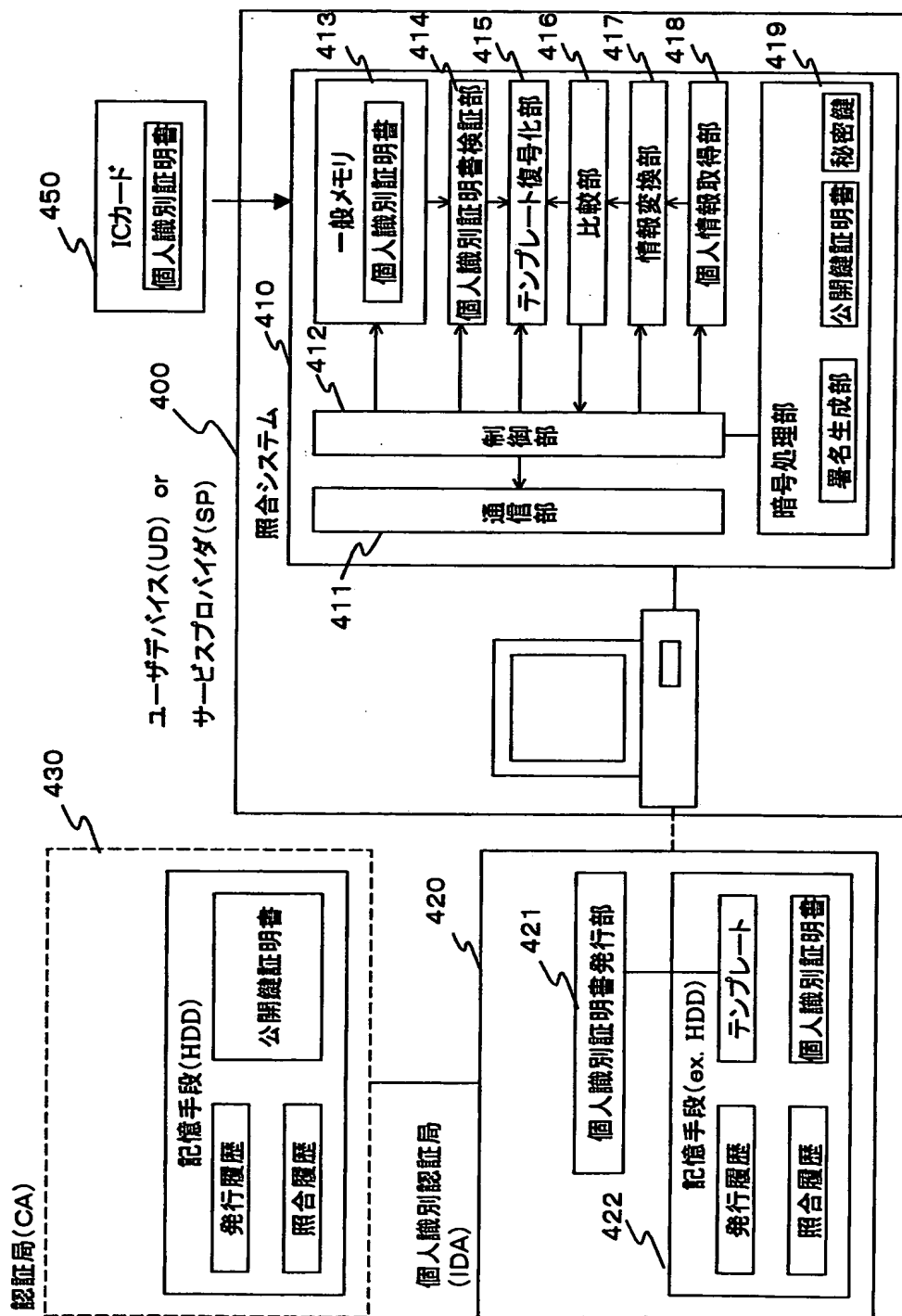
【図 18】



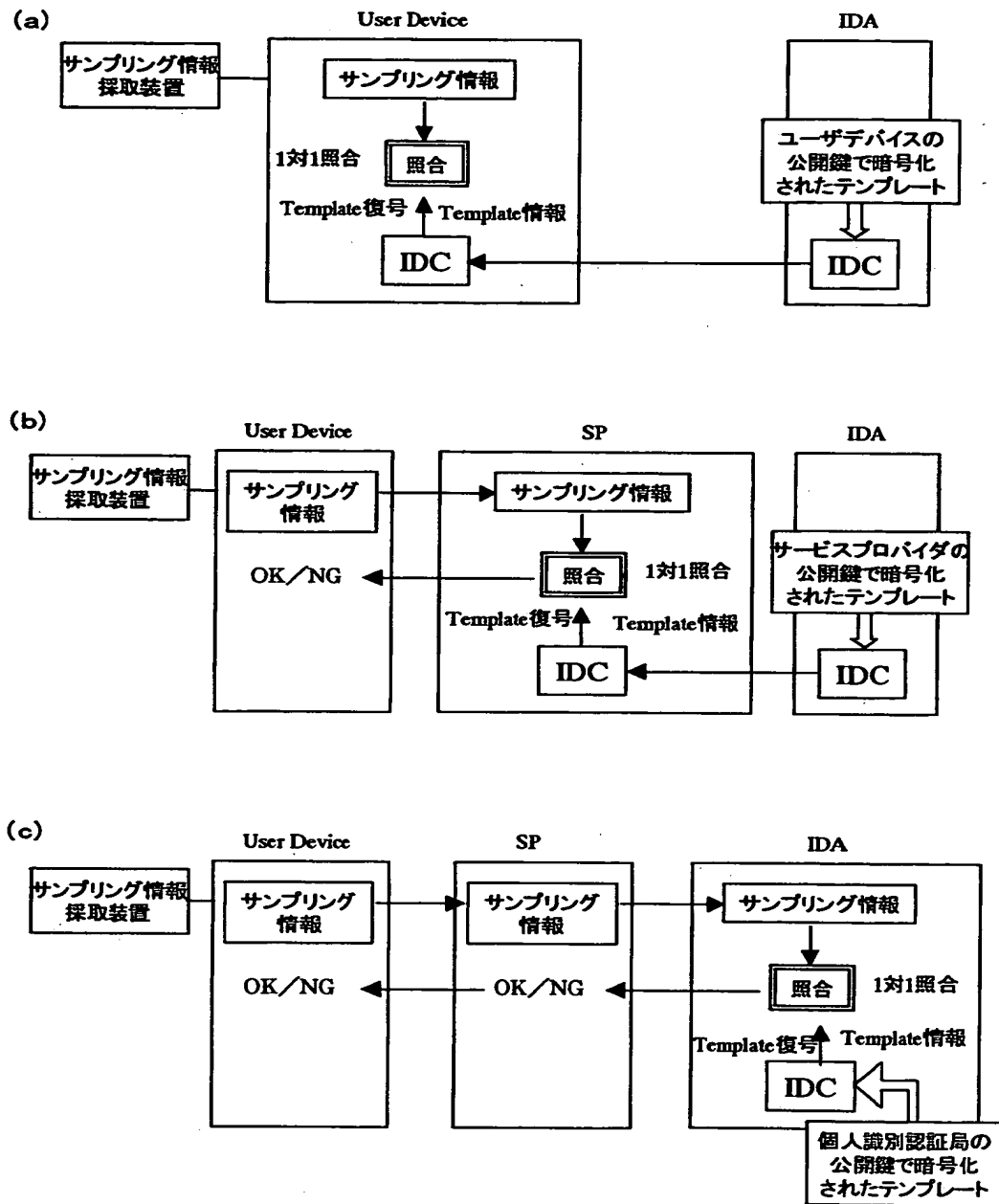
【図19】



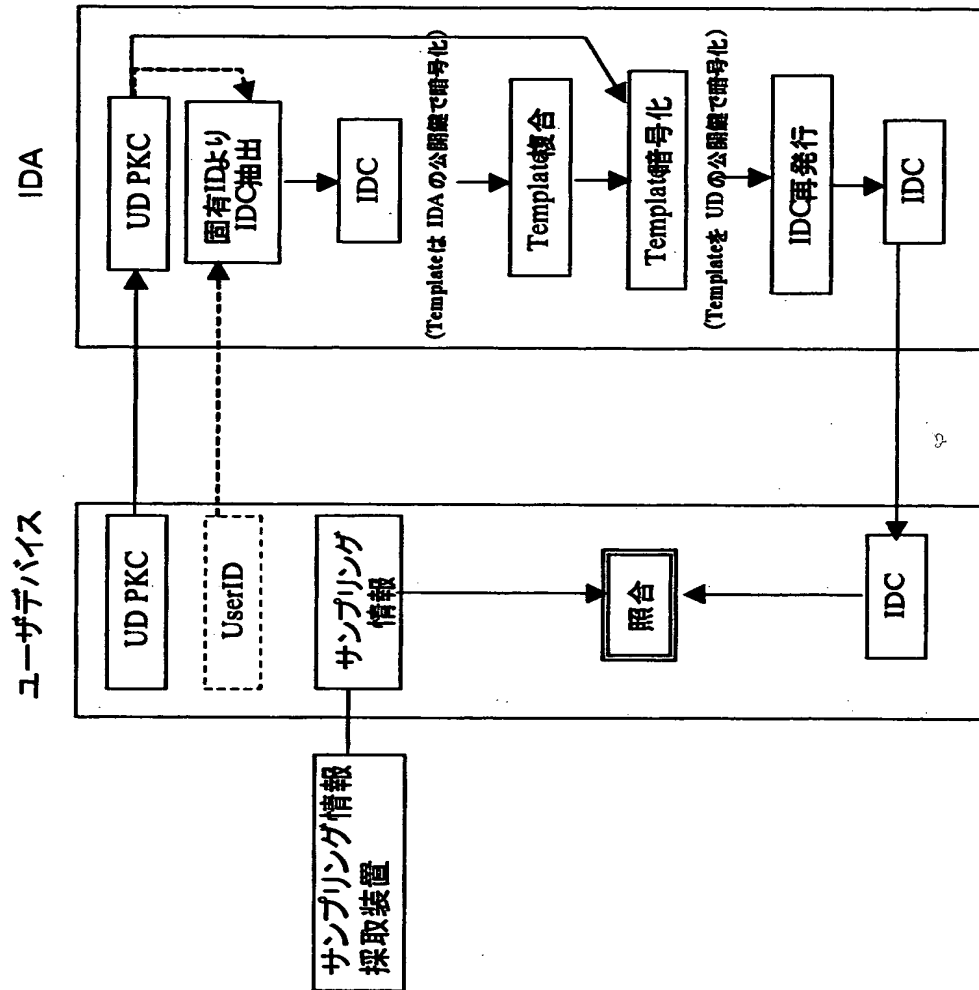
【図 20】



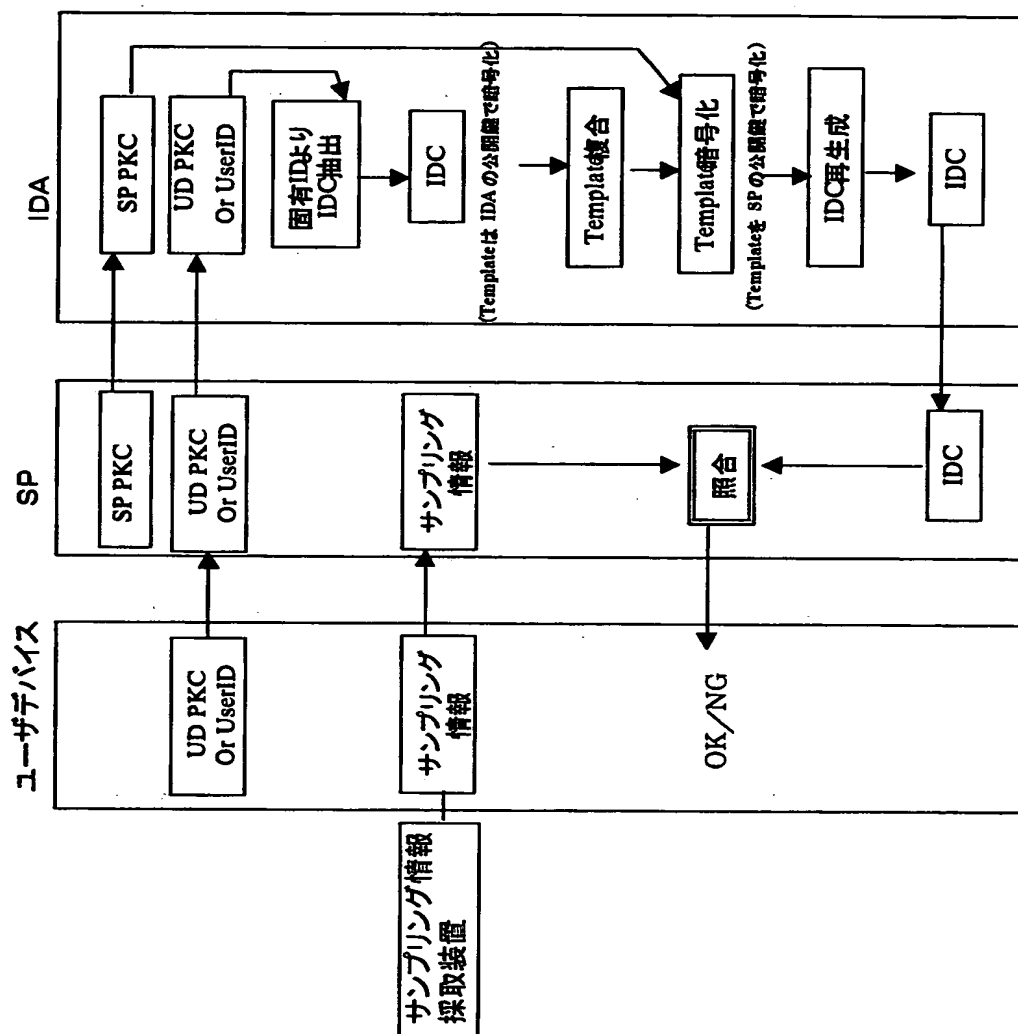
【図 2 1】



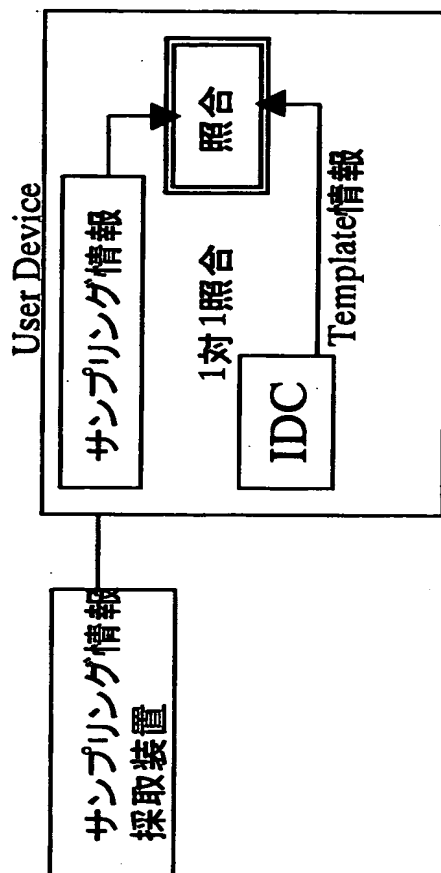
【図 22】



【図 23】

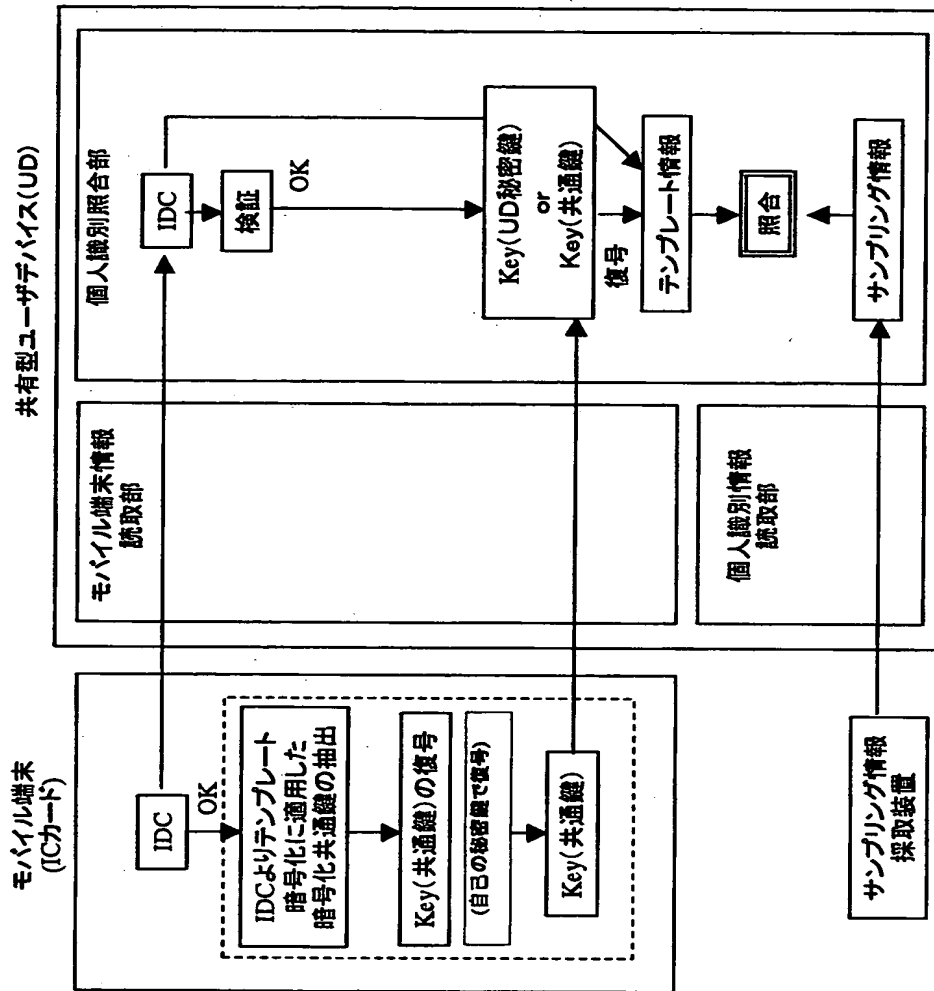


【図24】

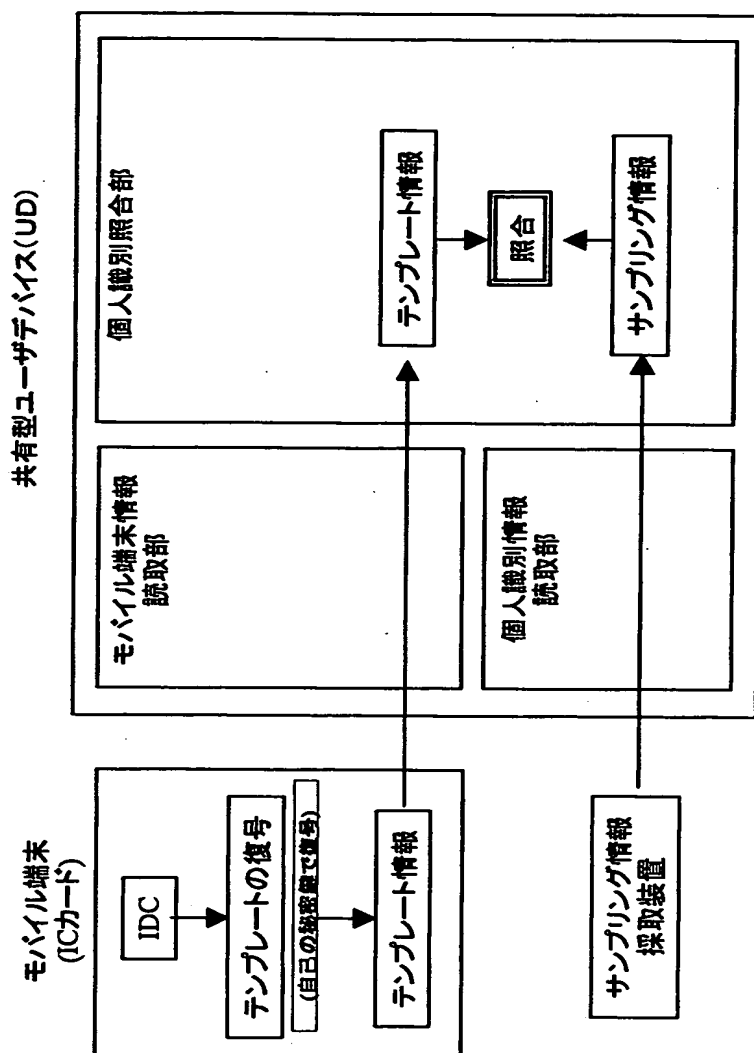




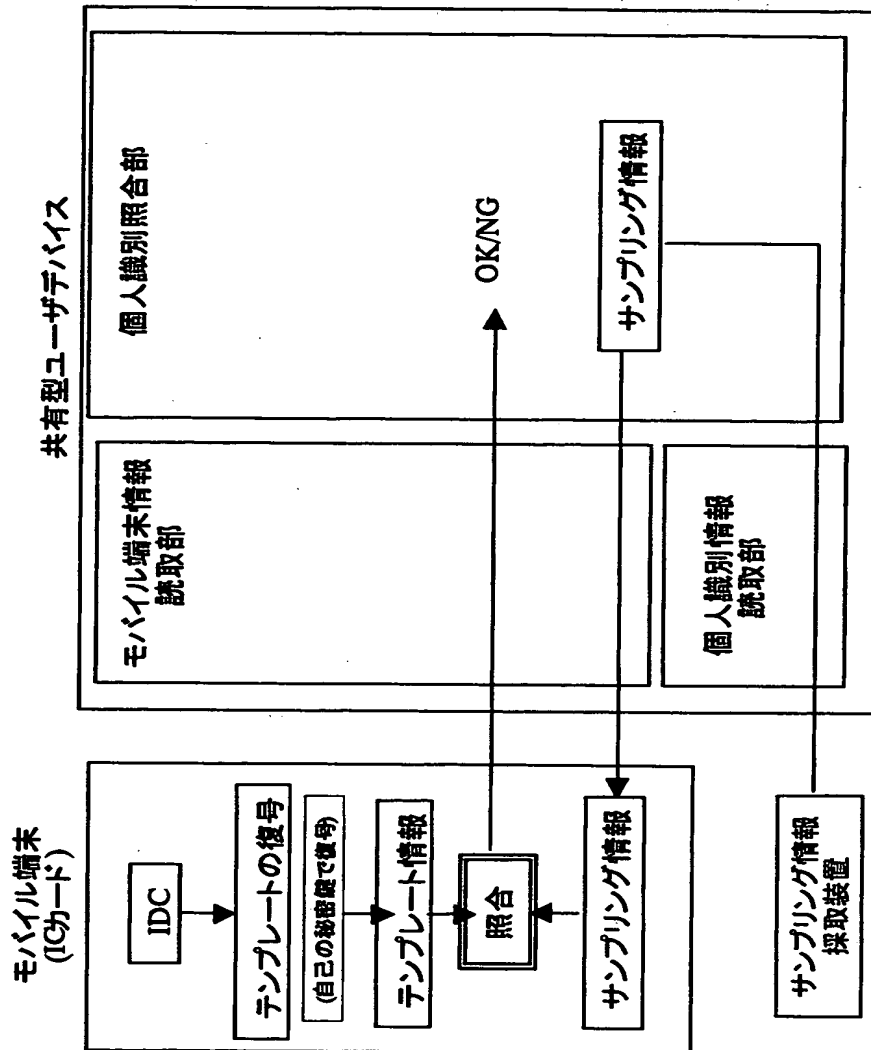
【図 25】



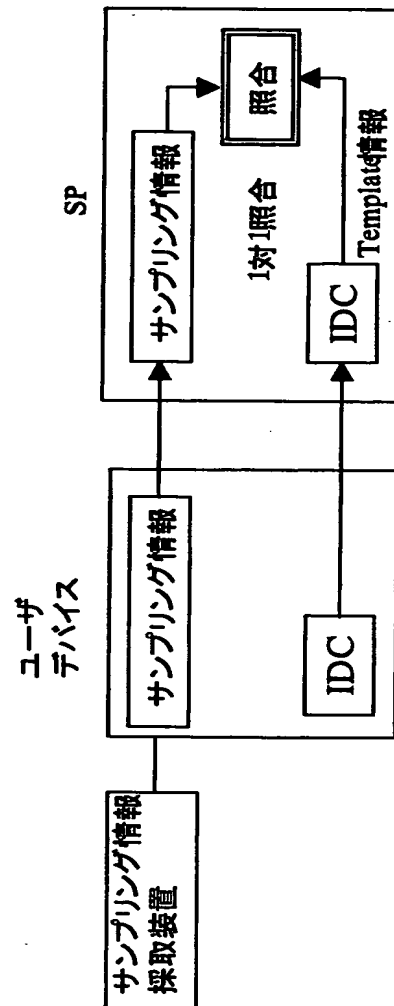
【図 26】



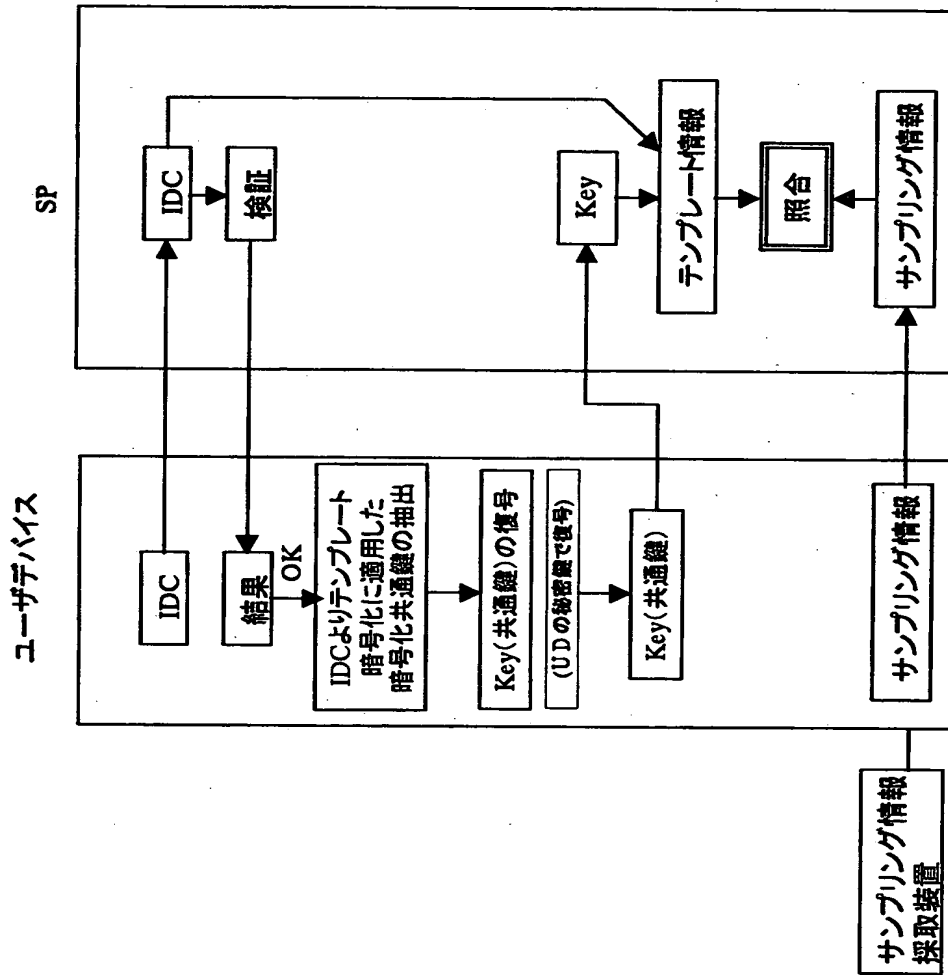
【図 27】



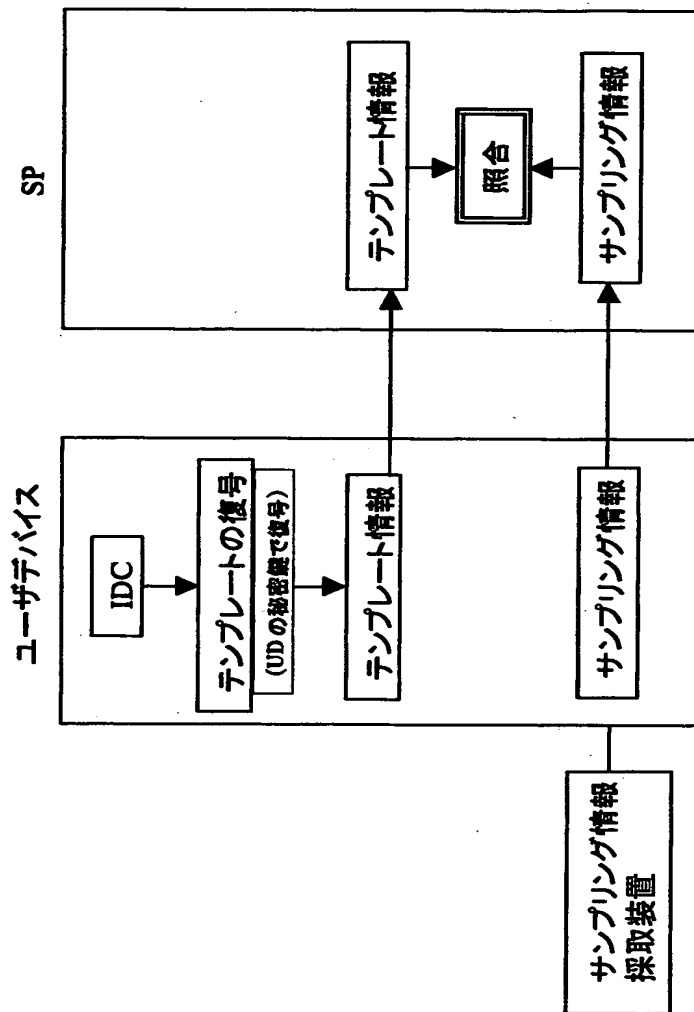
【図 2 8】



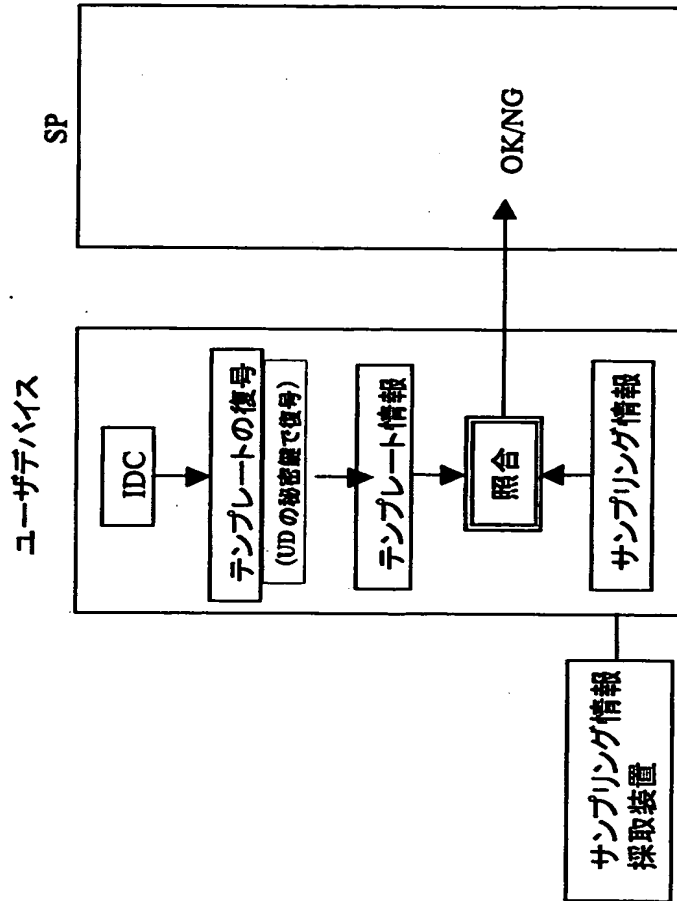
【図29】



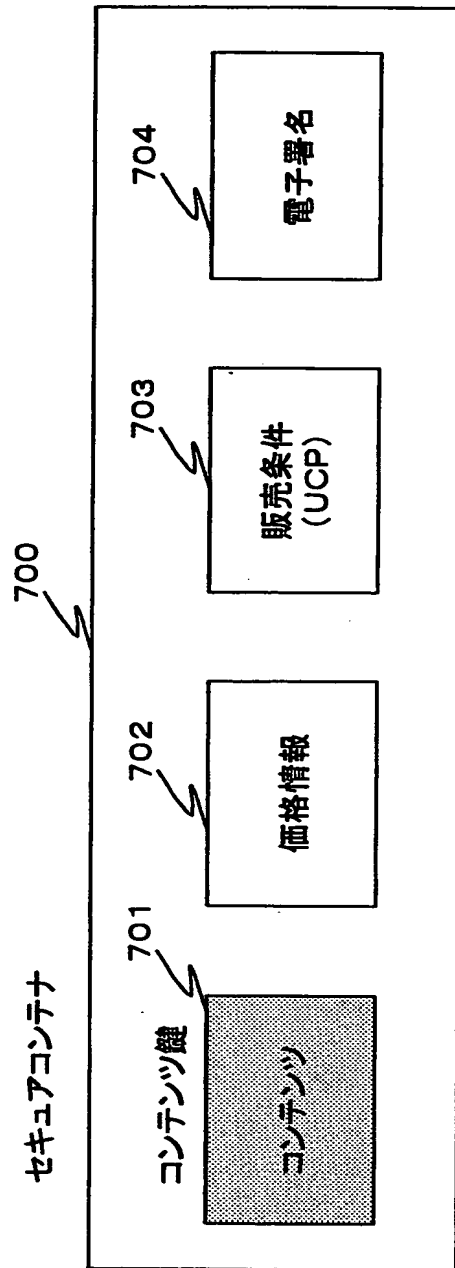
【図30】



【図 31】



【図 32】





【図 3 3】

IDC識別子リスト

| ユーザID   | 個人識別証明書(IDC)識別子 |
|---------|-----------------|
| ABC0001 | CDE00021        |
| ABC0002 | CDE00027        |
| ABC0003 | CDE03211        |
| :       | :               |
| BBC0231 | EED02333        |

【図 3 4】

|              |        |
|--------------|--------|
| データの種別       |        |
| 取扱方針の種類      |        |
| 取扱方針の有効期限    |        |
| コンテンツID      |        |
| コンテンツプロバイダID |        |
| 取扱方針ID       |        |
| 取扱方針バージョン    |        |
| 地域コード        |        |
| 使用可能機器条件     |        |
| 使用可能ユーザ条件    |        |
| IDC識別子リスト    |        |
| サービスプロバイダID  |        |
| UCP世代管理情報    |        |
| 二次配信可能回数     |        |
| ルール数         |        |
| ルールアドレス      |        |
| ルール<br>1     | ルール番号  |
|              | 利用権タイプ |
|              | :      |
| :            | :      |
| ルール<br>N     | ルール番号  |
|              | 利用権タイプ |
|              | :      |
| (署名検証の有無)    |        |
| 公開鍵証明書       |        |
| 署名           |        |

UCP(販売条件情報)

【図 3 5】

| ルール番号 | 利用権の内容       | 期間制限 | 回数制限 | 複製制限 |
|-------|--------------|------|------|------|
| 1     | 再生権          | なし   | なし   | —    |
| 2     |              | あり   | なし   | —    |
| 3     |              | なし   | あり   | —    |
| 4     | 複製権          | なし   | なし   | なし   |
| 5     |              | あり   | なし   | なし   |
| 6     |              | なし   | あり   | なし   |
| 7     |              | なし   | なし   | SCMS |
| 8     |              | あり   | なし   |      |
| 9     |              | なし   | あり   |      |
| 10    |              | なし   | なし   | その他  |
| 11    |              | あり   | なし   |      |
| 12    |              | なし   | あり   |      |
| 13    | 権利内容変更       |      |      |      |
| 14    | 再配布          |      |      |      |
| 15    | アルバム化アップグレード |      |      |      |
| 16    | 管理移動権        |      |      |      |

【図 36】

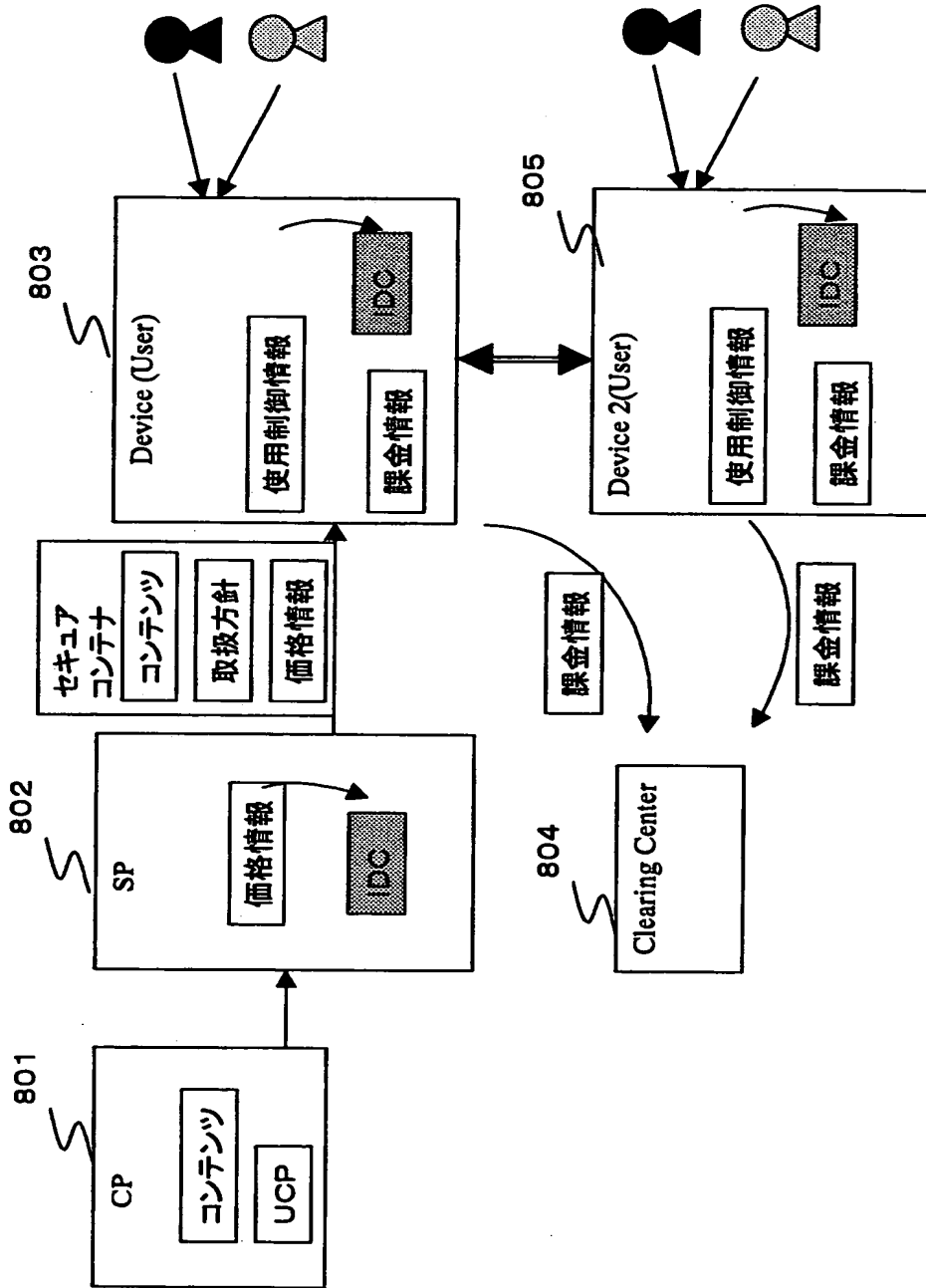
|              |       |
|--------------|-------|
| データの種別       |       |
| 価格情報の種類      |       |
| 価格情報の有効期限    |       |
| コンテンツID      |       |
| サービスプロバイダID  |       |
| 価格情報ID       |       |
| 価格情報バージョン    |       |
| 地域コード        |       |
| 使用可能機器条件     |       |
| 使用可能ユーザ条件    |       |
| IDC識別子リスト    |       |
| コンテンツプロバイダID |       |
| 取扱方針ID       |       |
| ルール数         |       |
| ルールアドレス      |       |
| ルール1         | ルール番号 |
|              | :     |
|              | :     |
| :            | :     |
| ルールN         | ルール番号 |
|              | :     |
|              | :     |
| (署名検証の有無)    |       |
| 公開鍵証明書       |       |
| 署名           |       |

721

価格情報

【図 37】

IDCを利用したコンテンツの権利処理



【図 3 8】

|                 |
|-----------------|
| データの種別          |
| 使用許諾条件情報の種類     |
| 使用許諾条件情報の有効期限   |
| コンテンツID         |
| アルバムID          |
| 暗号処理部ID         |
| ユーザID           |
| コンテンツプロバイダID    |
| 取扱方針ID          |
| 取扱方針バージョン       |
| サービスプロバイダID     |
| 価格情報ID          |
| 価格情報のバージョン      |
| 使用許諾条件情報のID     |
| 再生権(利用権)のルール番号  |
| 利用権内容番号         |
| 再生残り回数          |
| 再生権の有効期限        |
| 複製権(利用権)のルール番号  |
| 利用権内容番号         |
| 複製残り回数          |
| UCS世代管理情報       |
| UCS二次配信可能回数     |
| IDC識別子リスト       |
| 再生権を保有する暗号処理部ID |

732

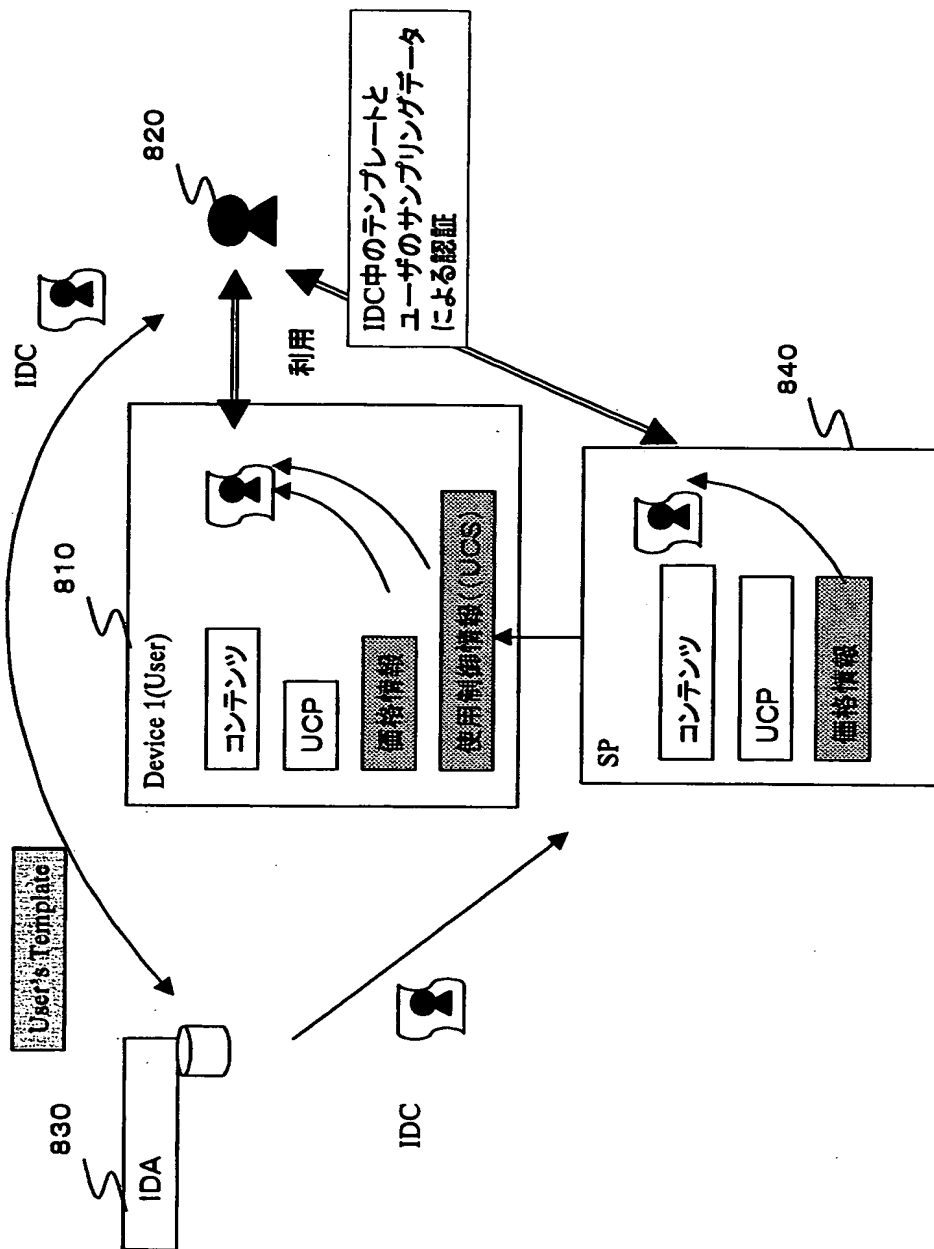
733

731

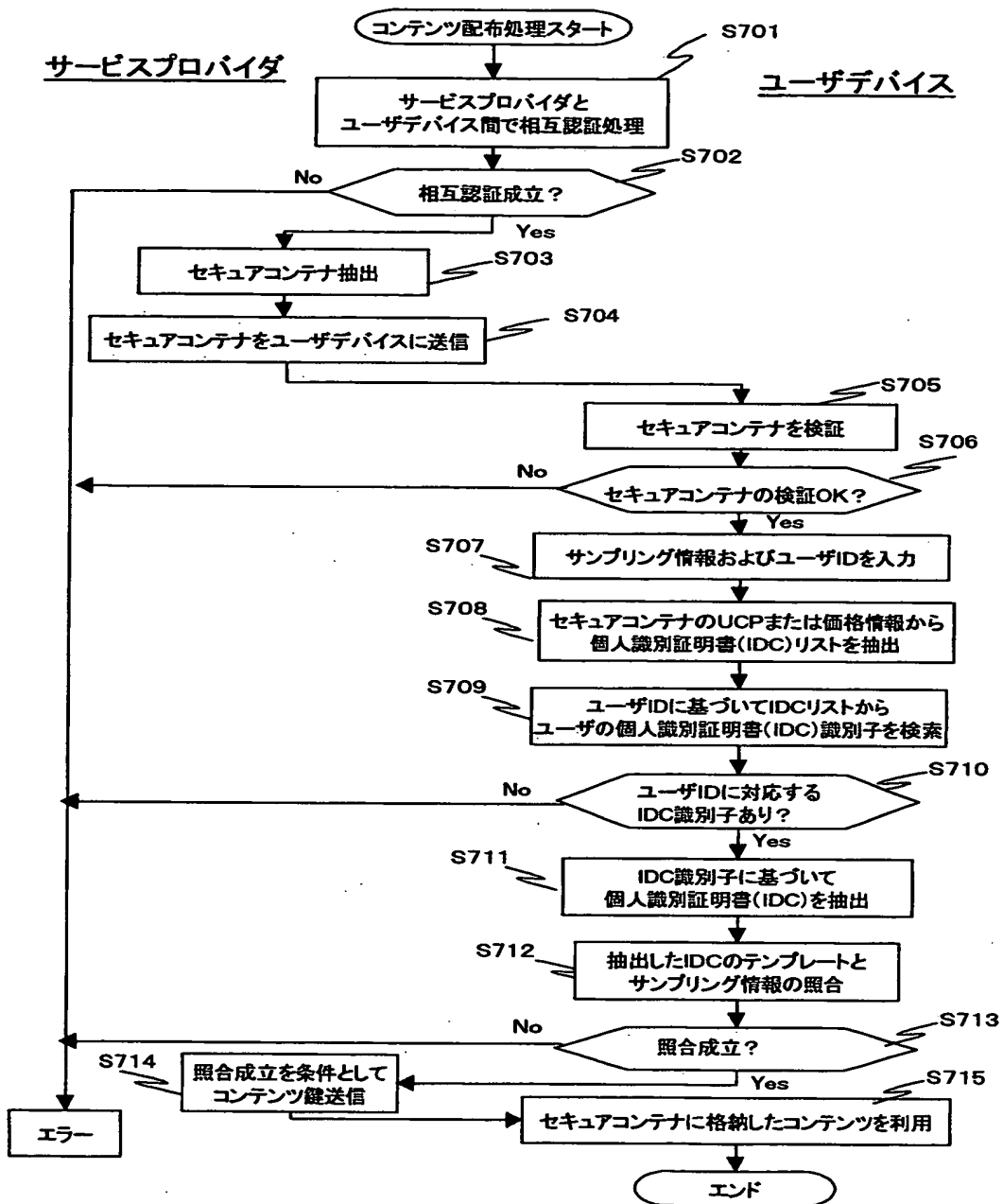
UCS(使用制御情報)

【図 39】

IDCを利用したコンテンツの権利処理

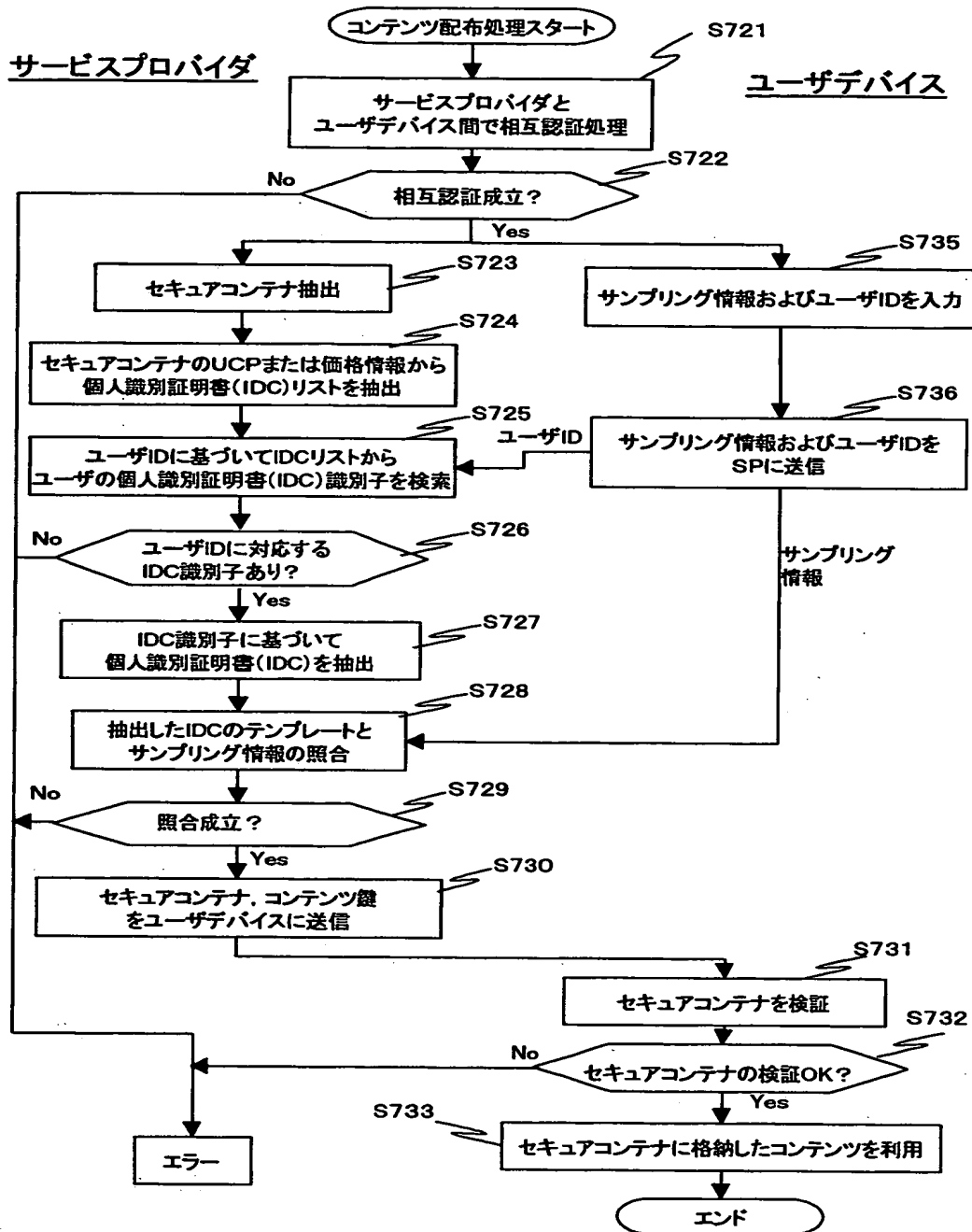


【図40】

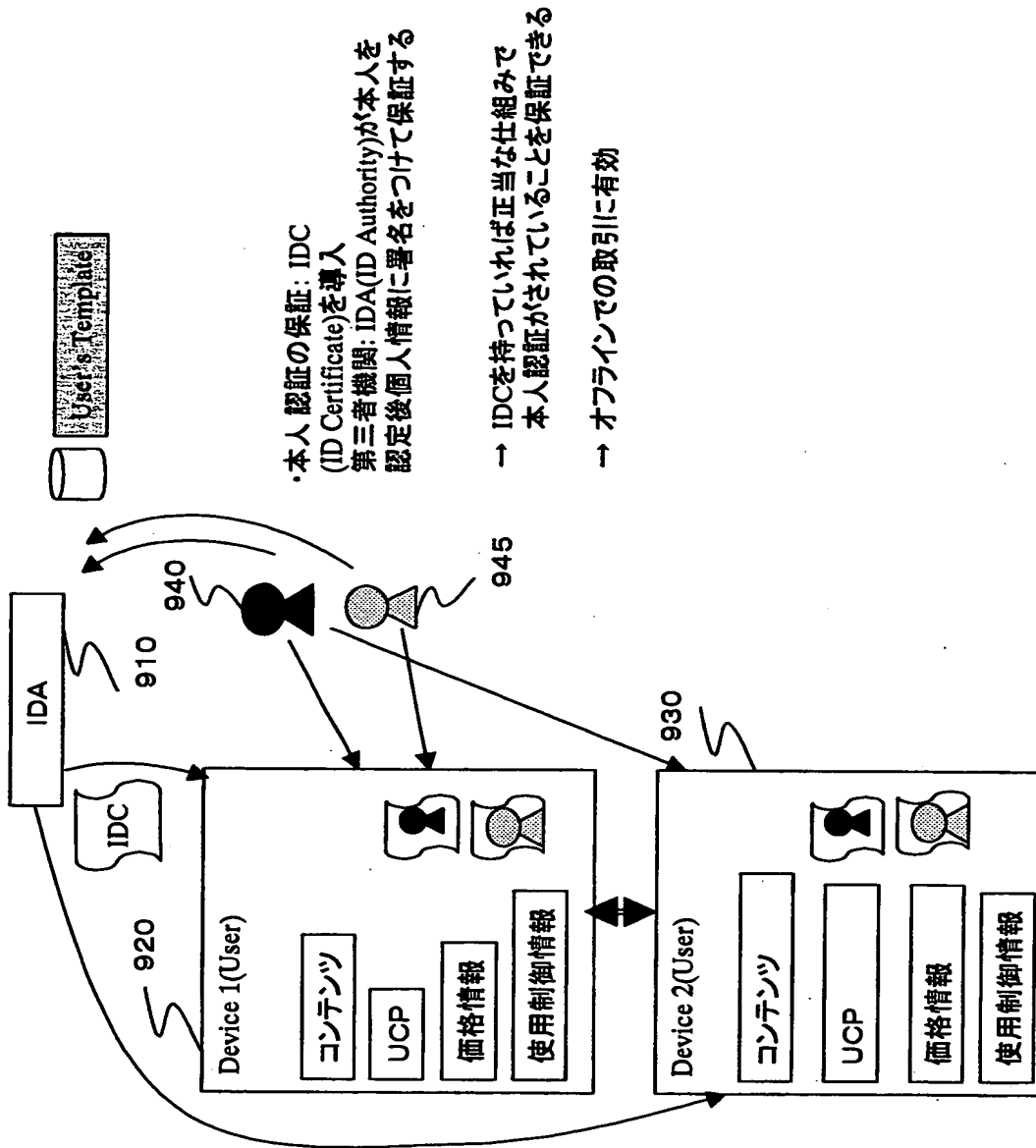




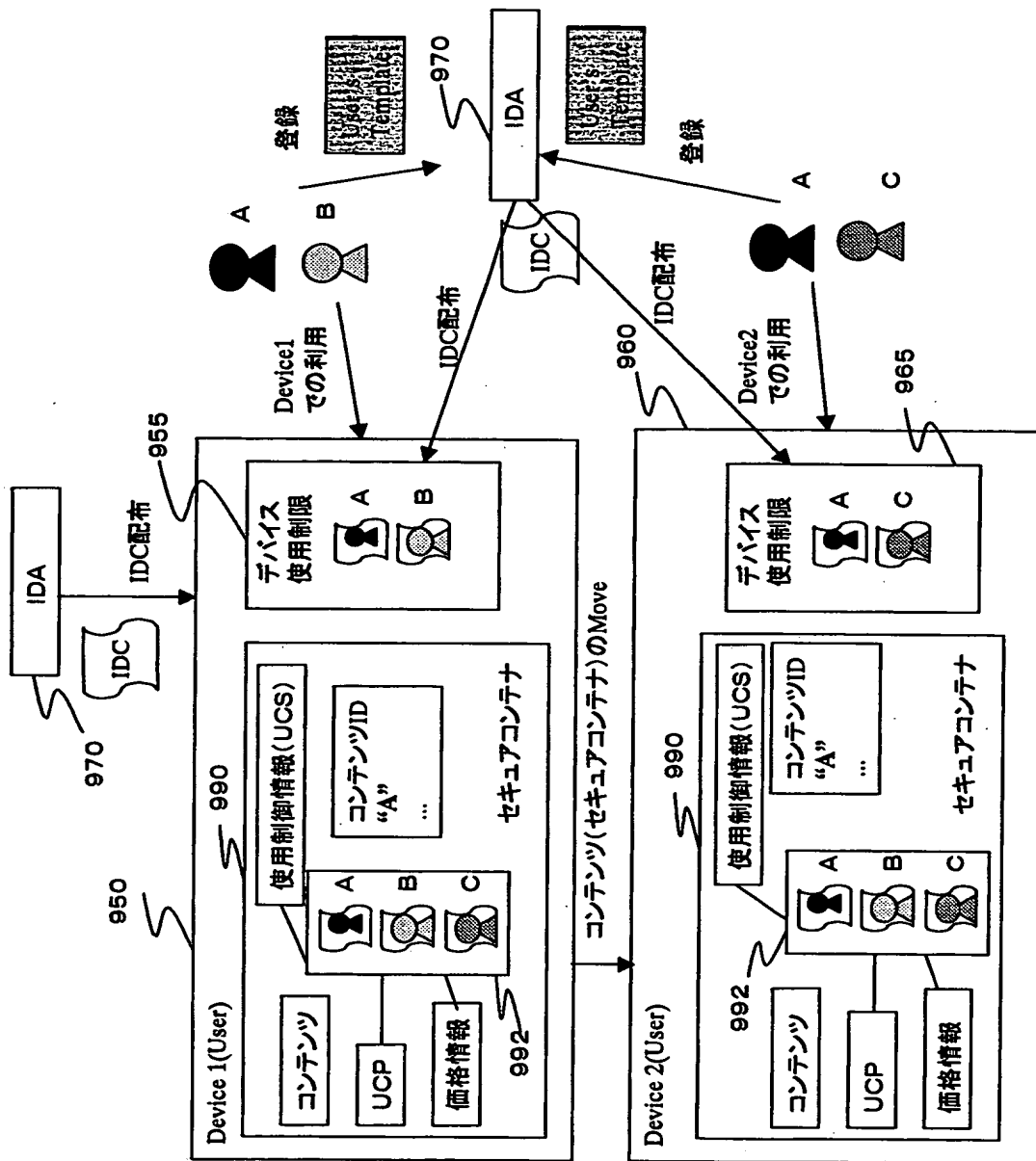
【図 41】



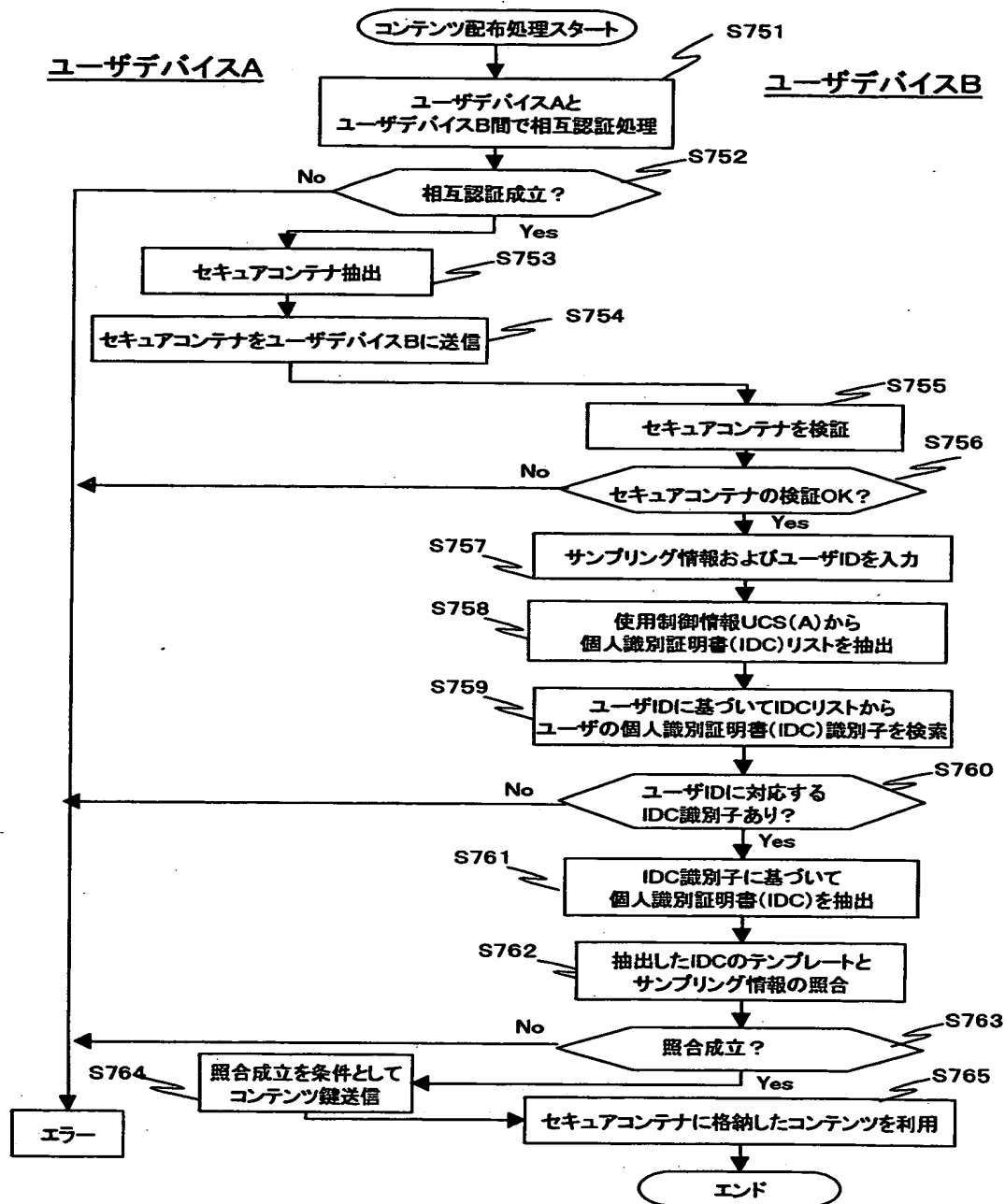
【図 4 2】



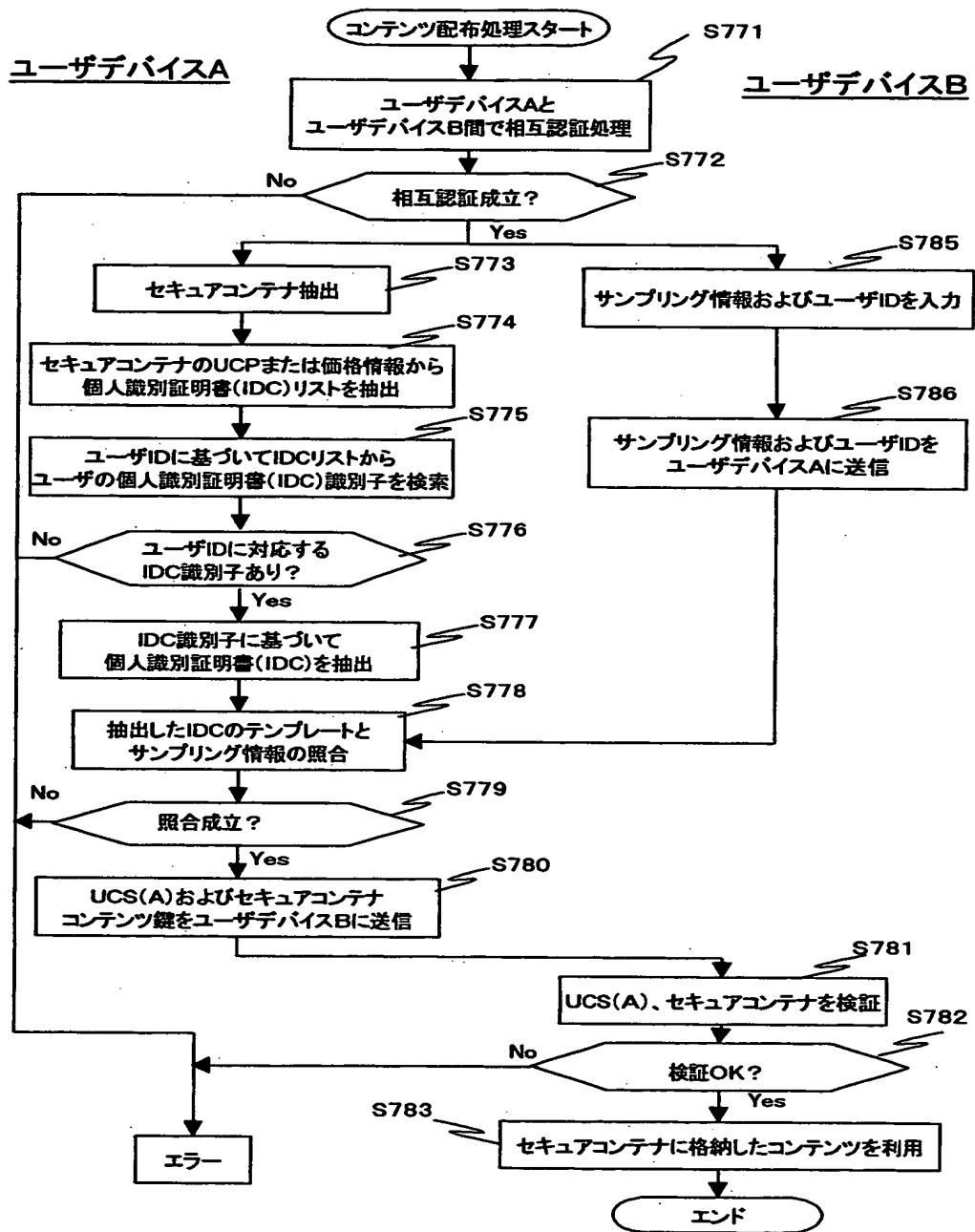
【図43】



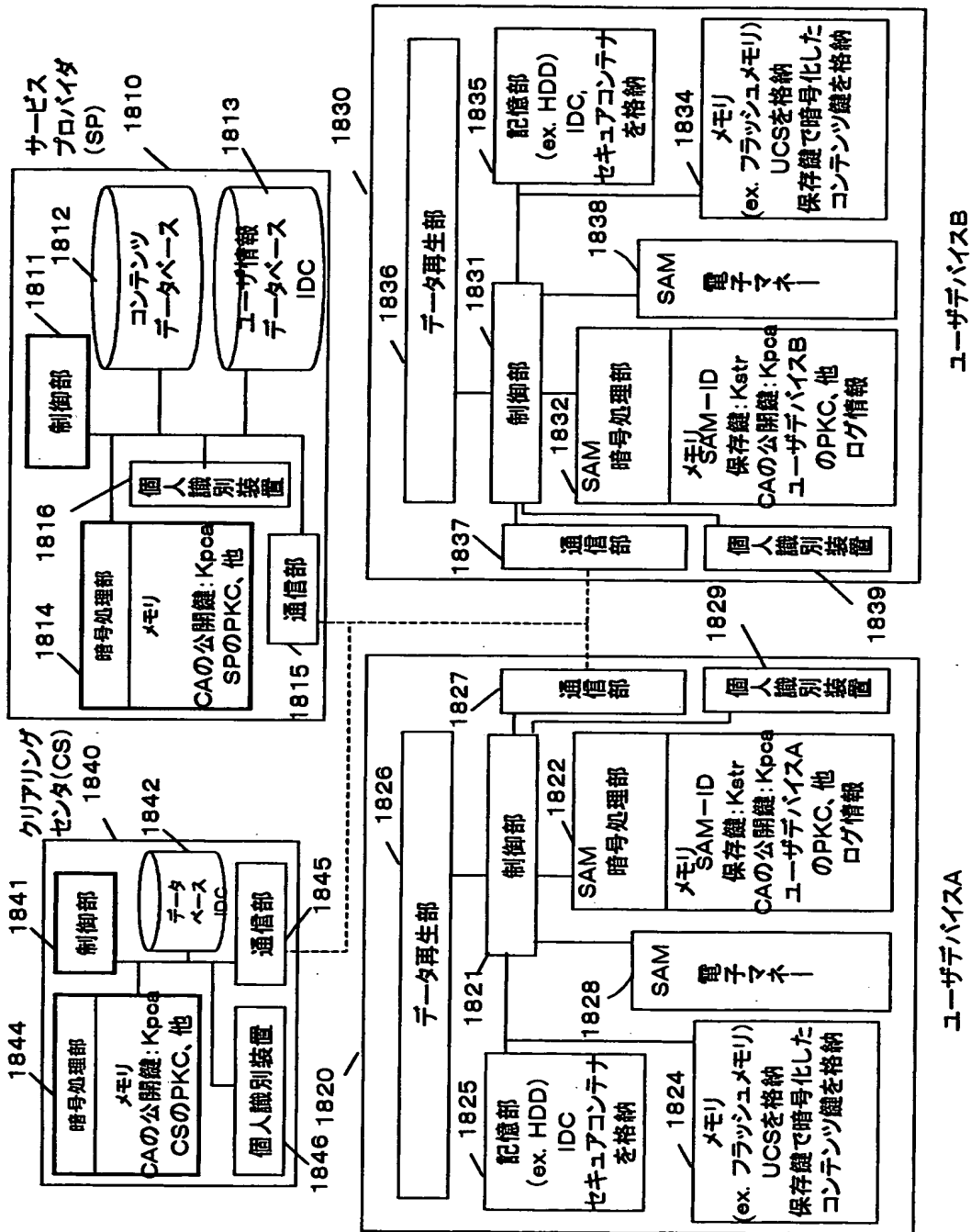
【図44】



【図45】

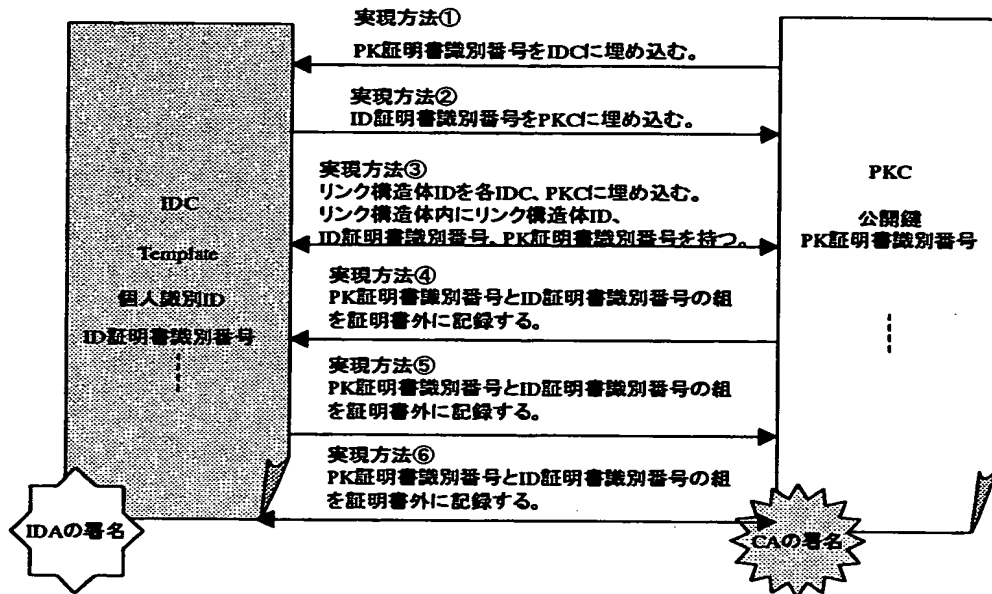


【图 4 6】

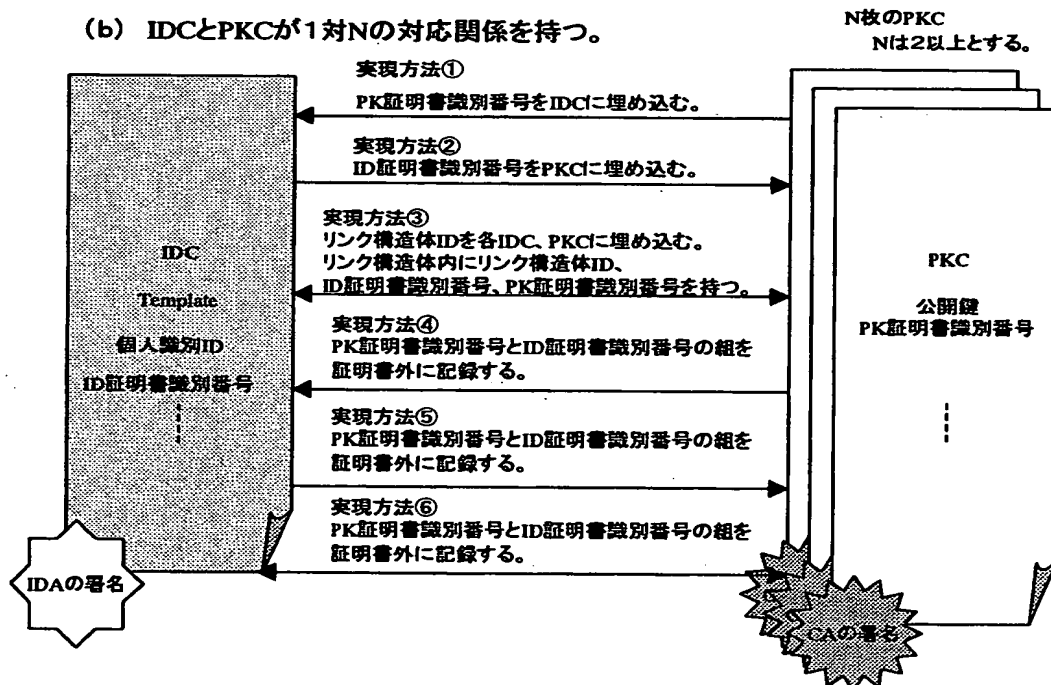


【図 4 7】

(a) IDCとPKCが1対1の対応関係を持つ。

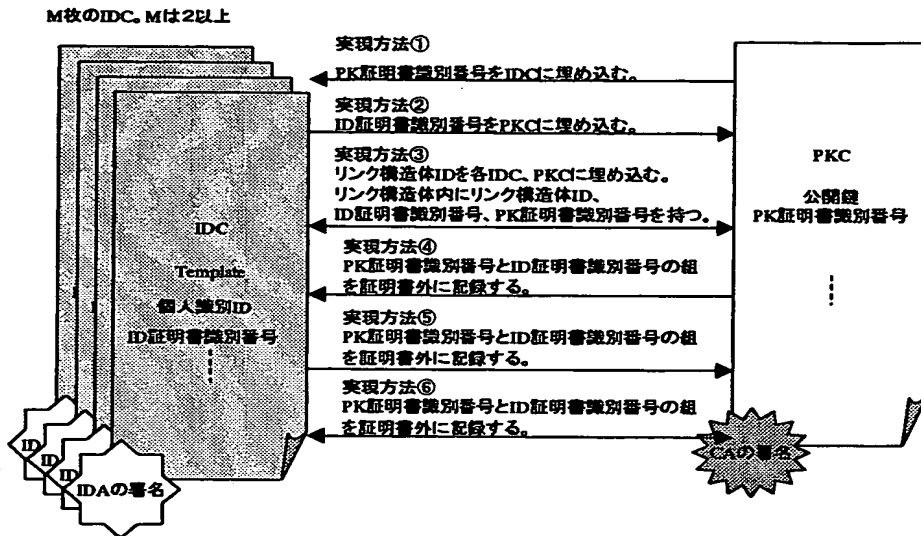


(b) IDCとPKCが1対Nの対応関係を持つ。

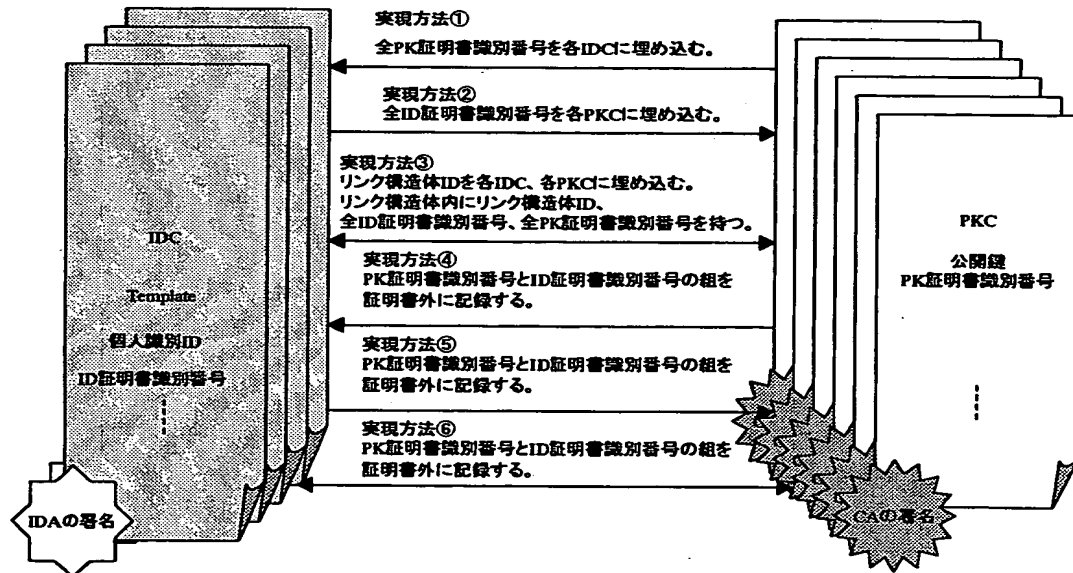


【図 48】

(c) IDCとPKCがM対1の対応関係を持つ。

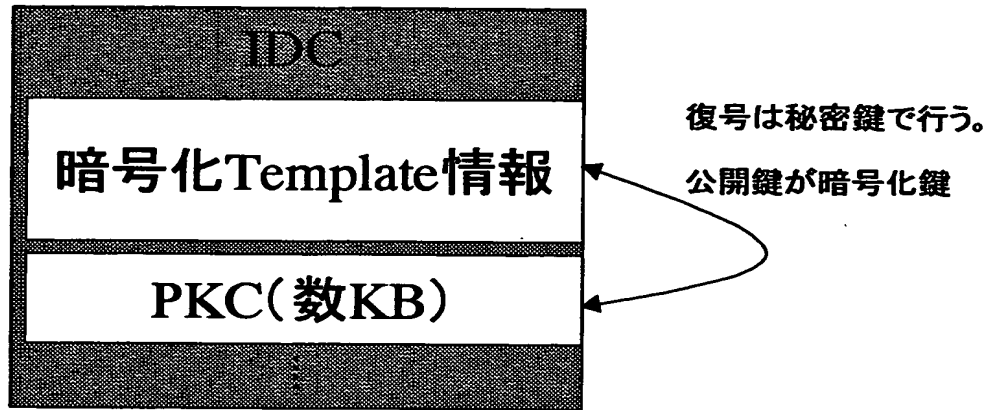


(d) IDCとPKCがM対Nの対応関係を持つ。

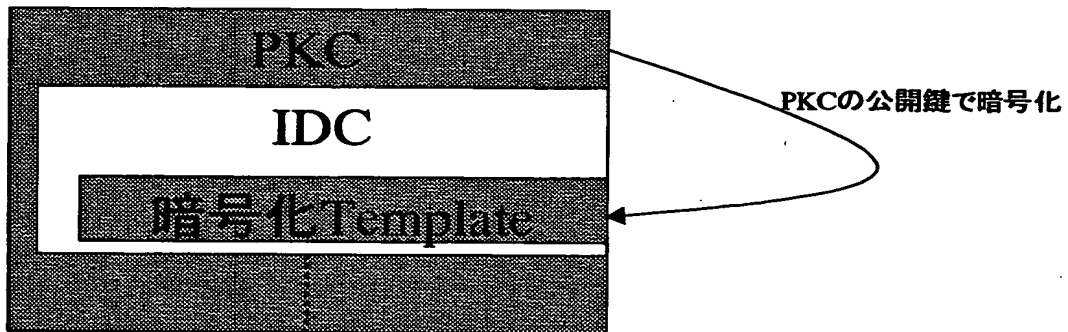




【図 4 9】

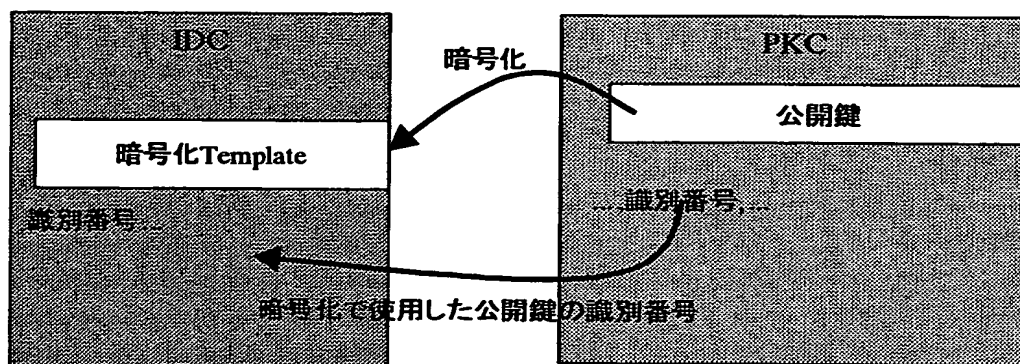


(a)

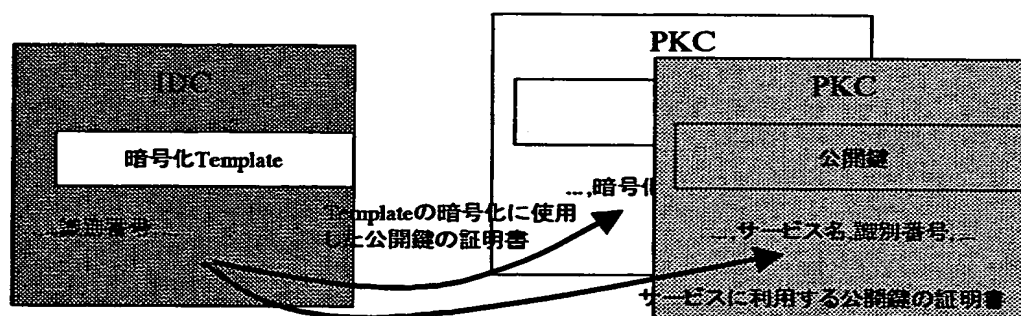


(b)

【図 50】

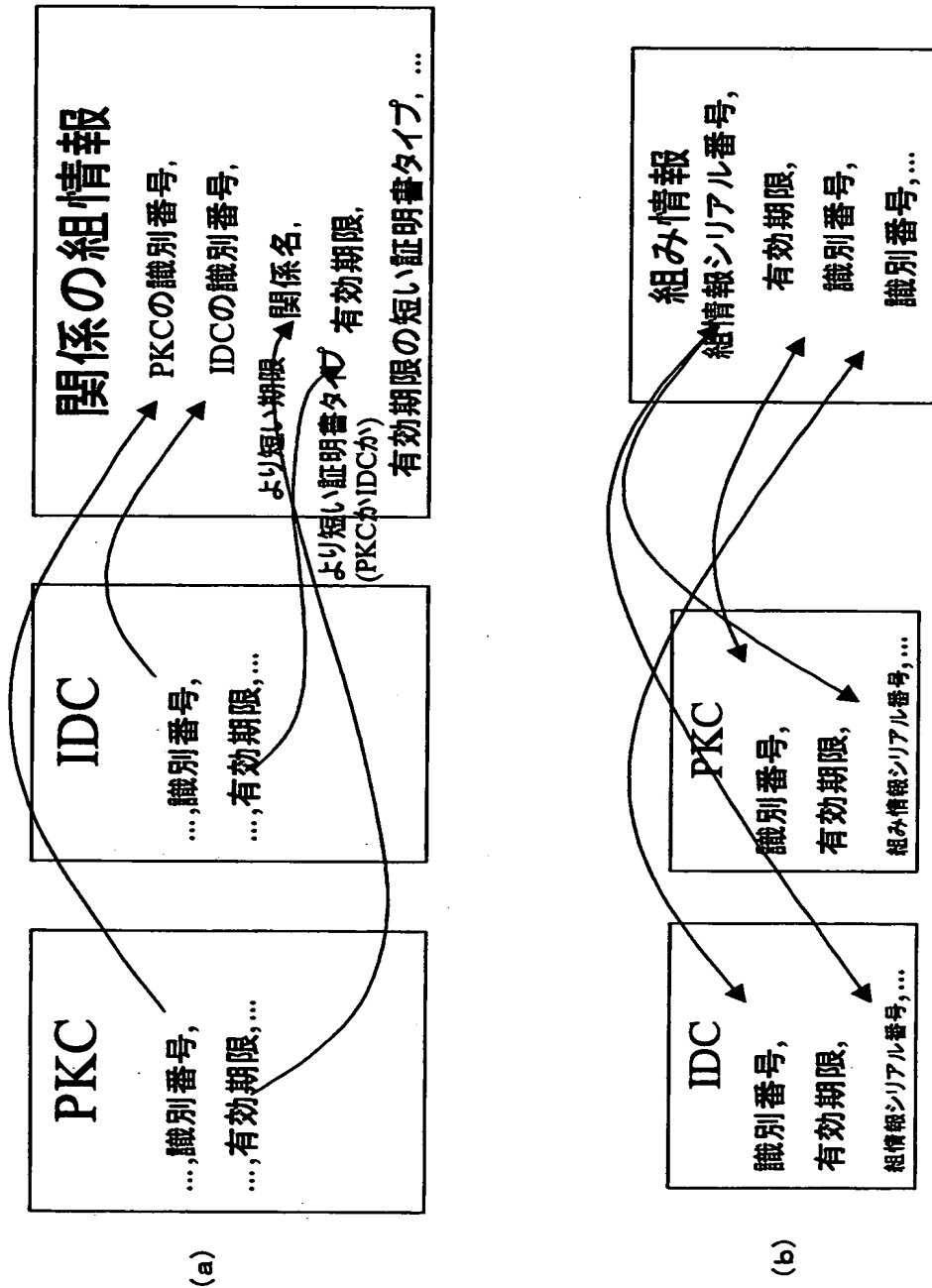


(a)

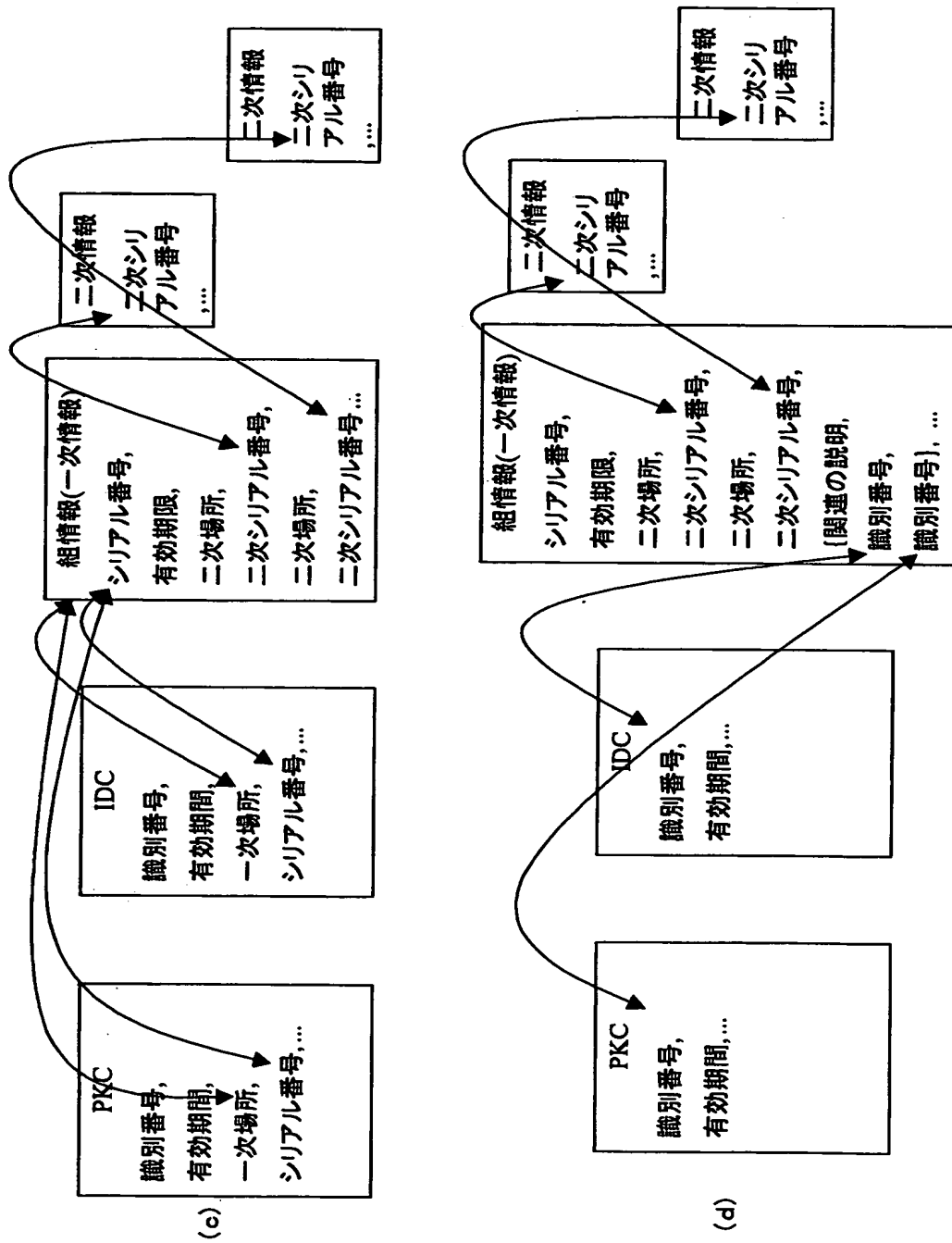


(b)

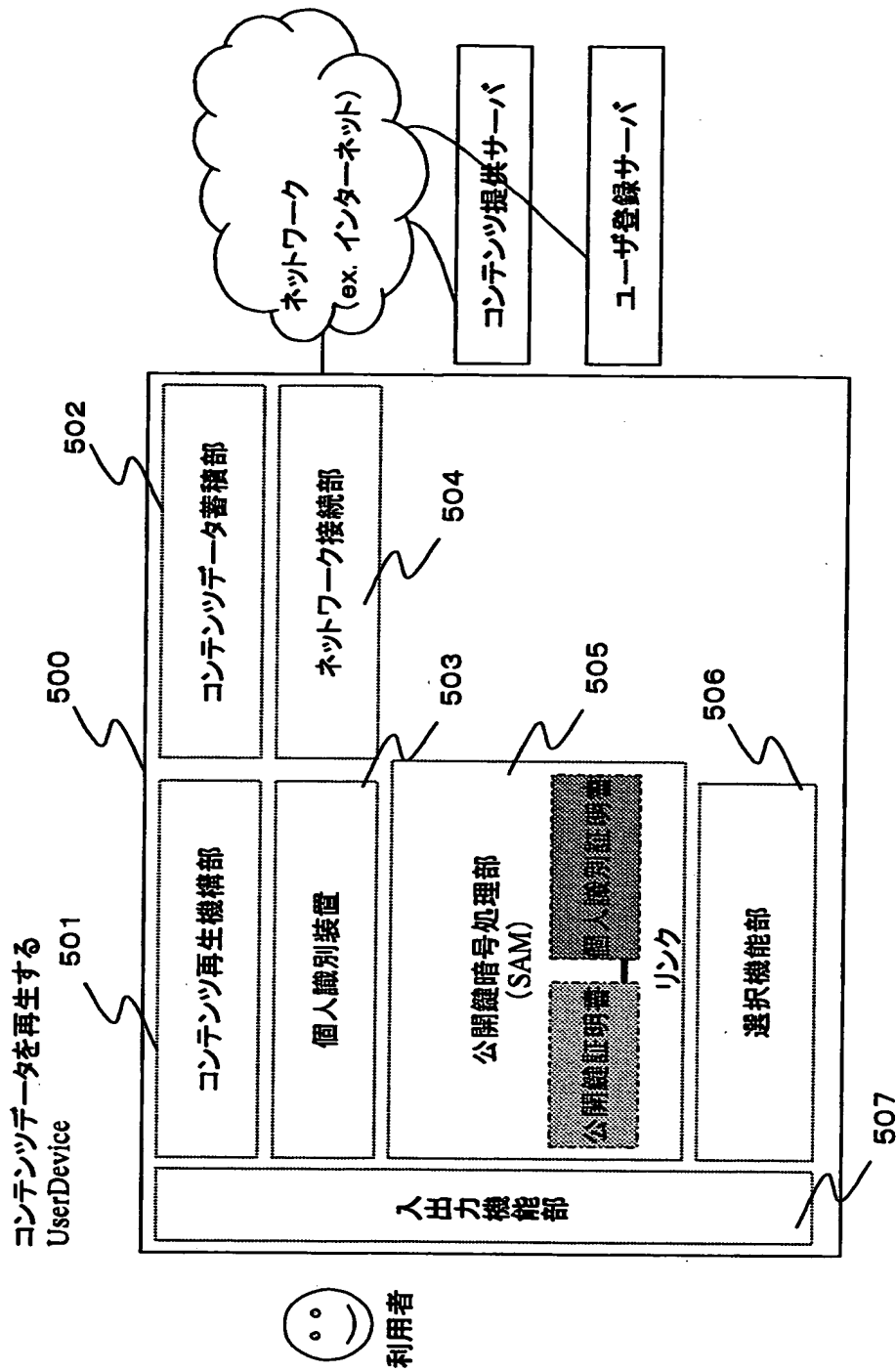
【図 5 1】



【図 5 2】



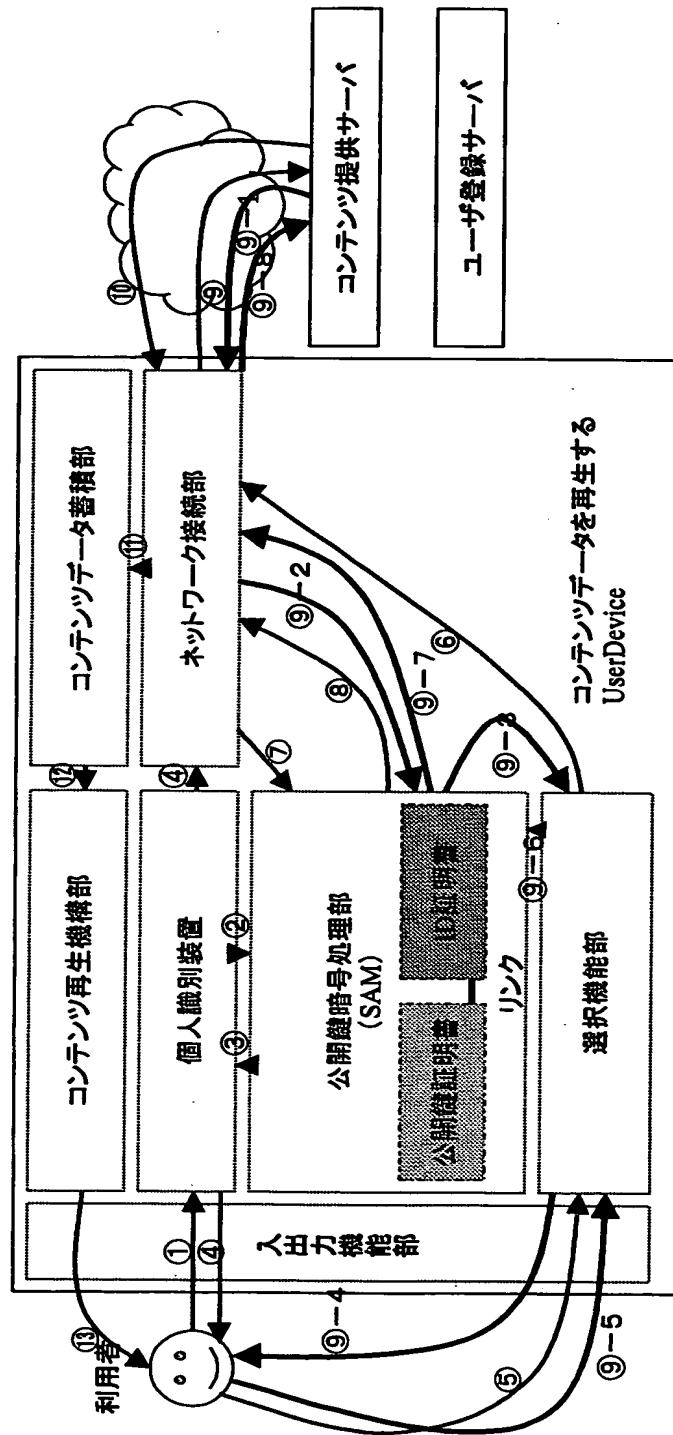
【図 53】



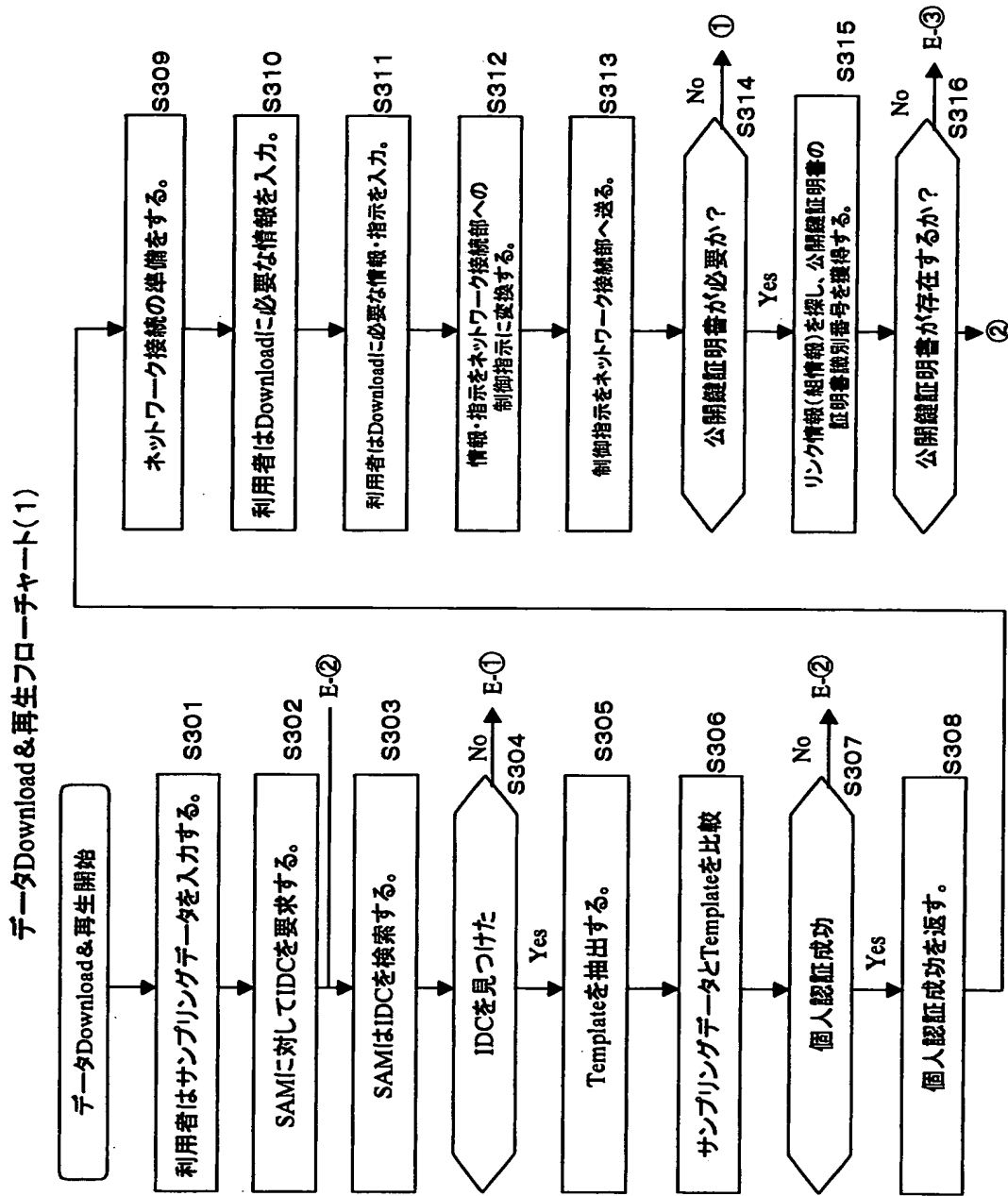
【図 5 4】

## データDownload&amp;再生

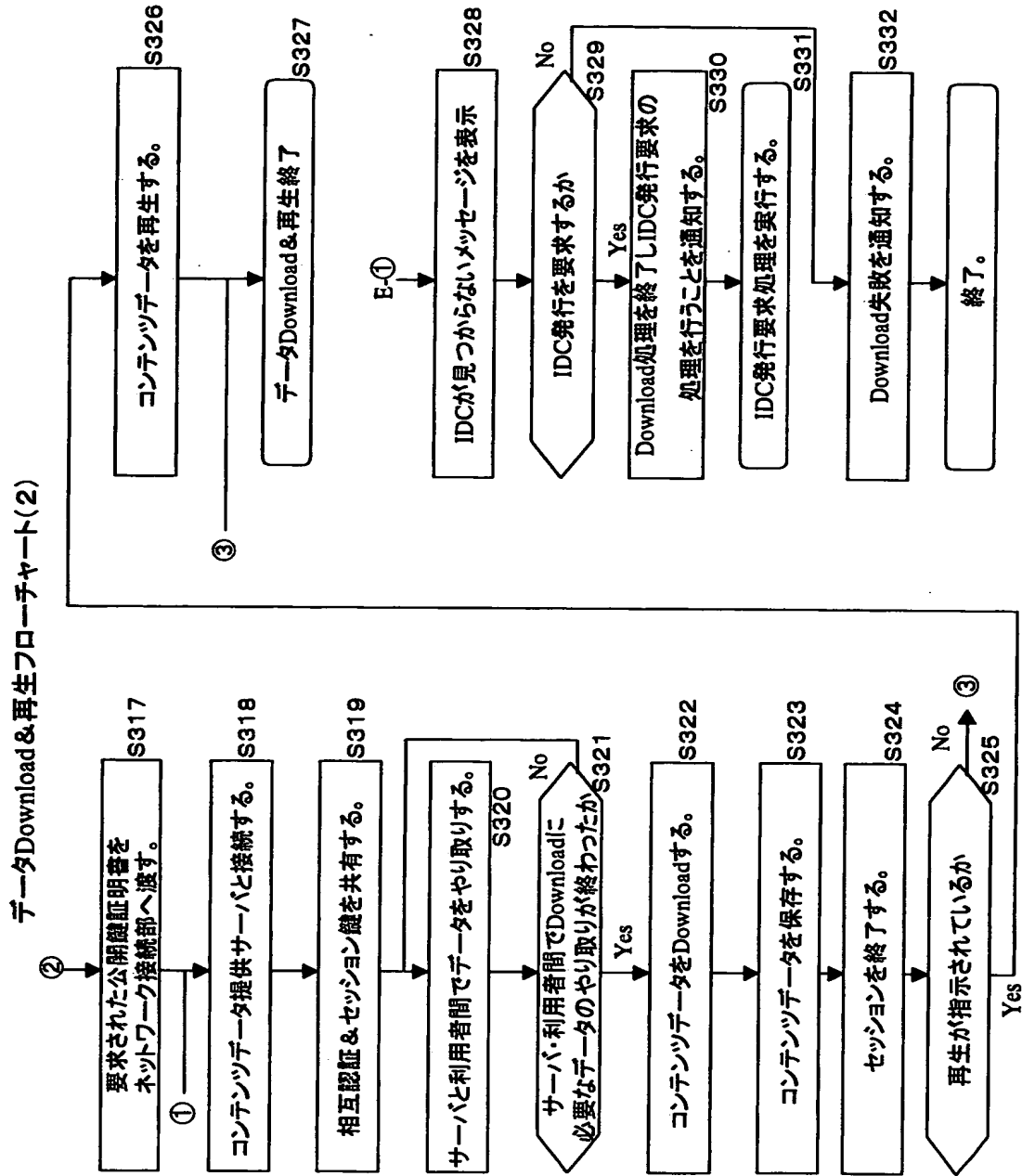
- 前提条件:
  - 既にIDCとPKCを獲得している。
  - コンテンツ提供サーバに対して必要なユーザ登録は終わっている。



【図 55】



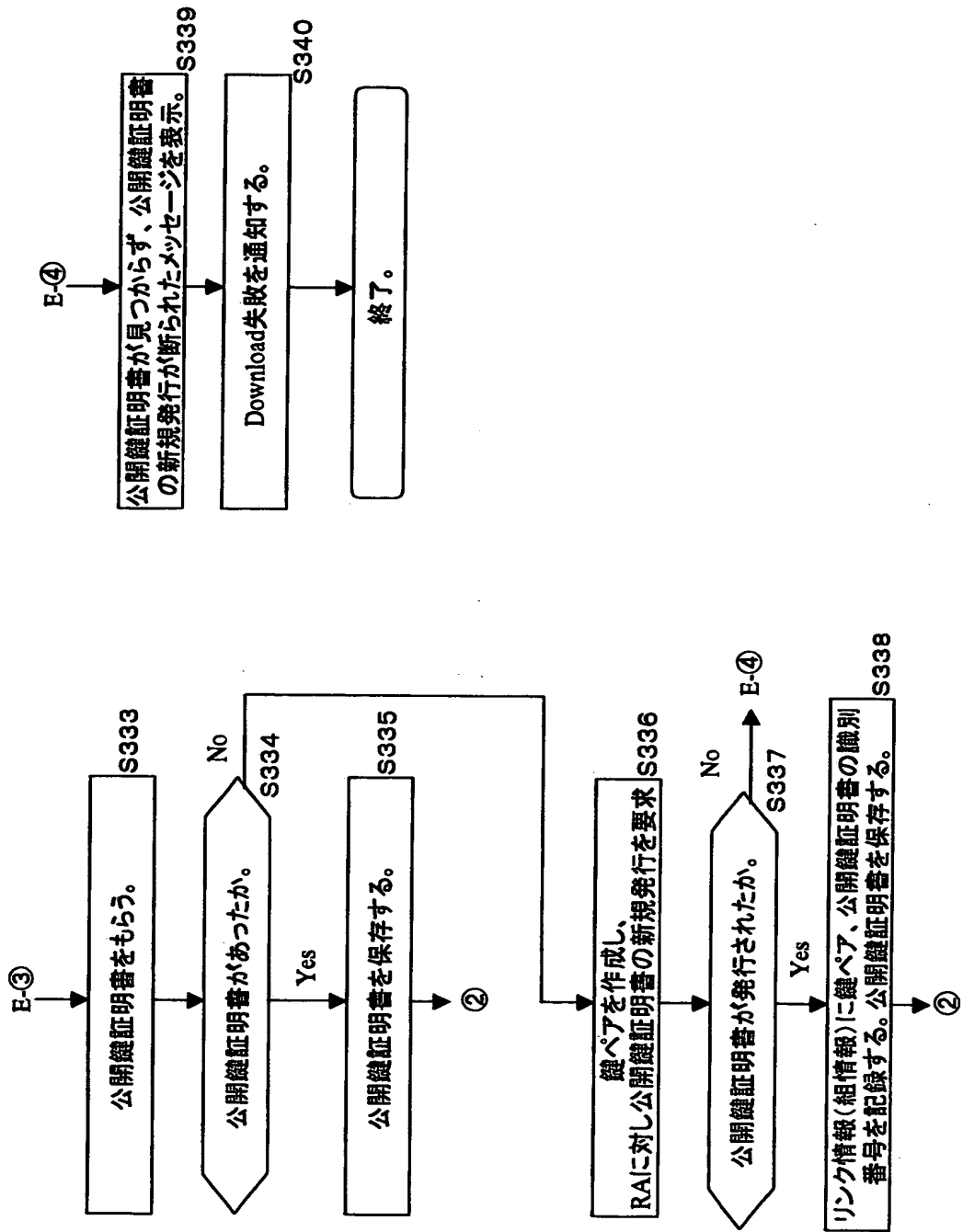
【図 5 6】





【図 57】

データDownload & 再生フローチャート(3)

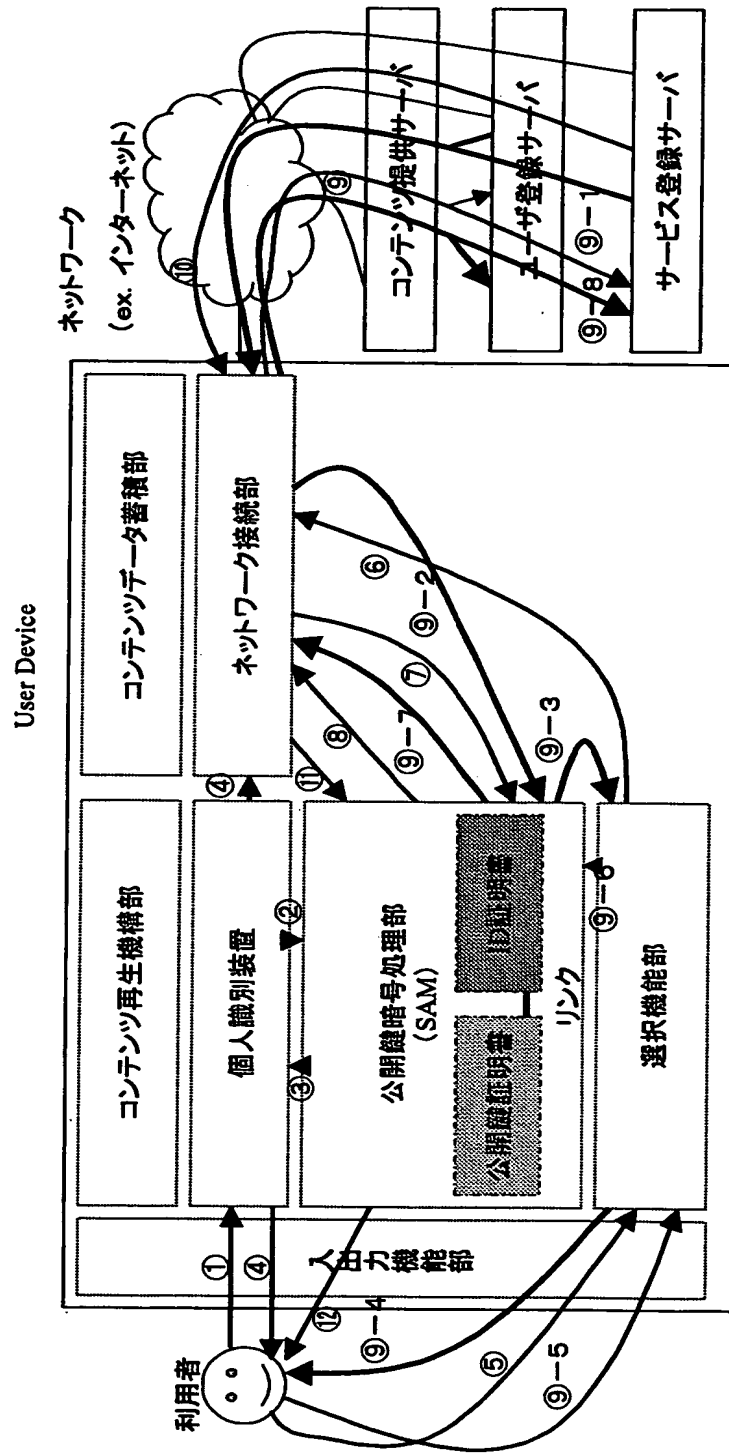


【図58】

ユーザ登録、ユーザ登録抹消、サービス契約における処理の流れ

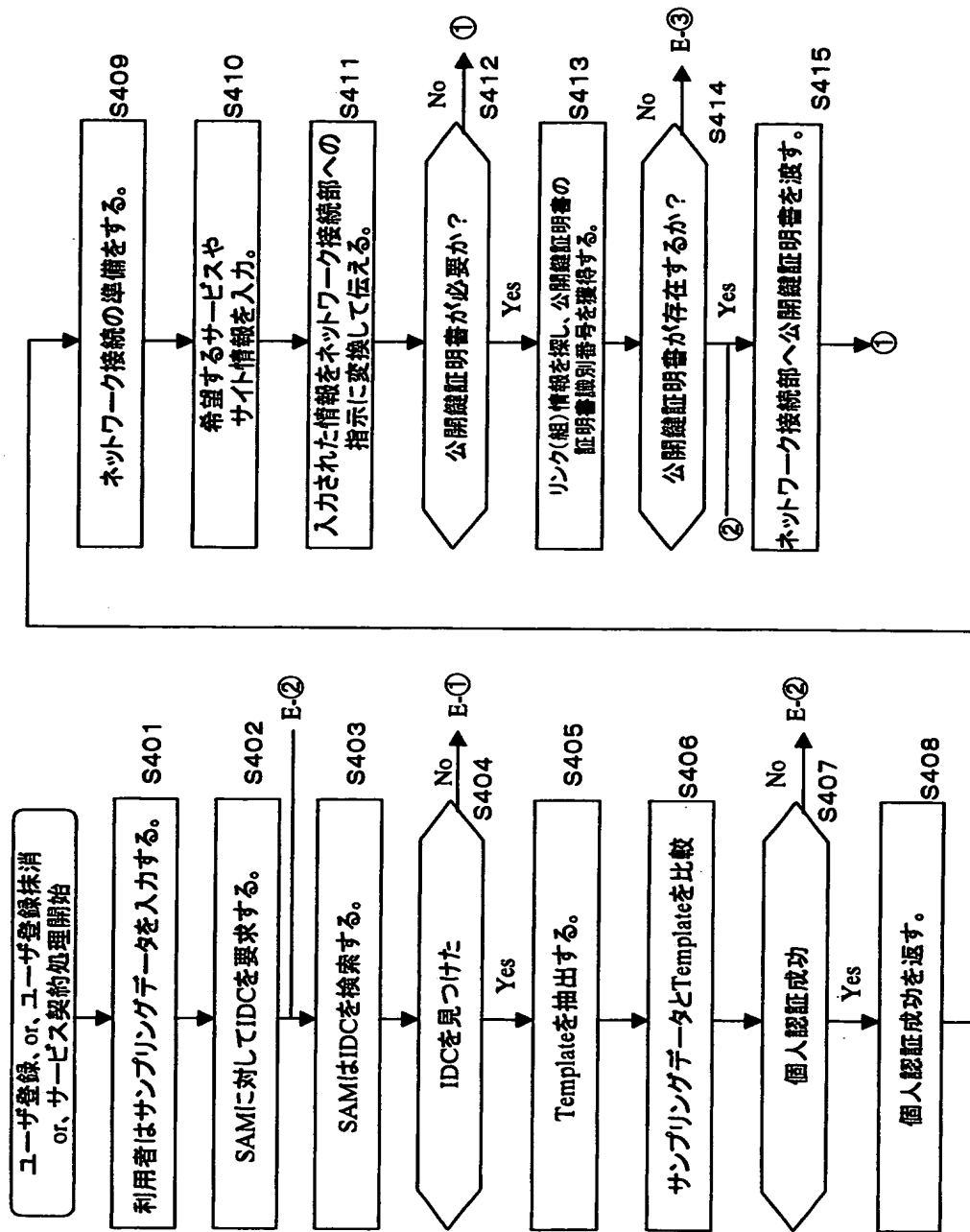
・ 前提条件:

- 既にIDCとPKCを獲得している。



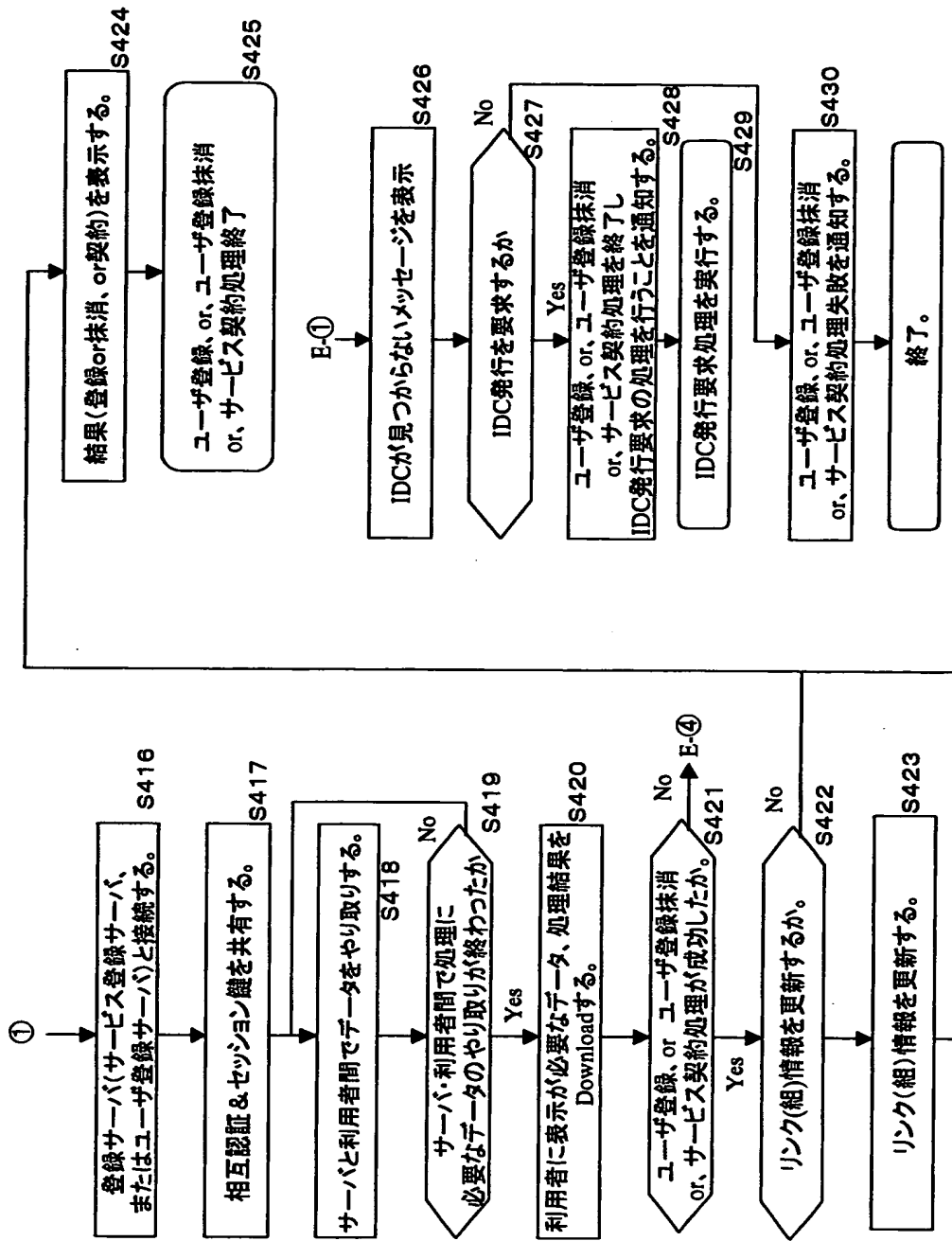
【図 59】

ユーザ登録、抹消、サービス契約におけるフローチャート(1)



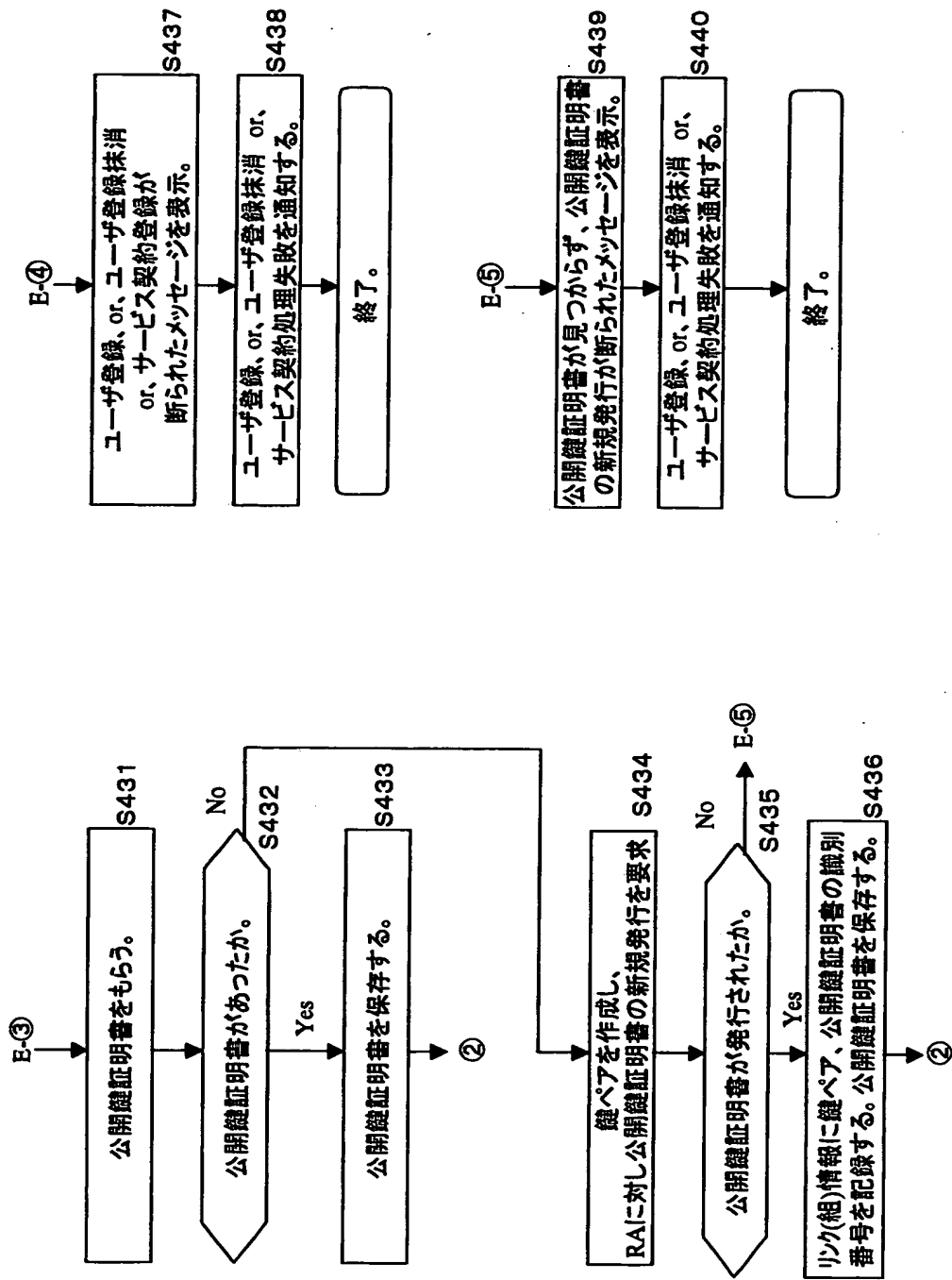
【図 6 0】

## ユーザ登録、抹消、サービス契約におけるフローチャート(2)



【図 6 1】

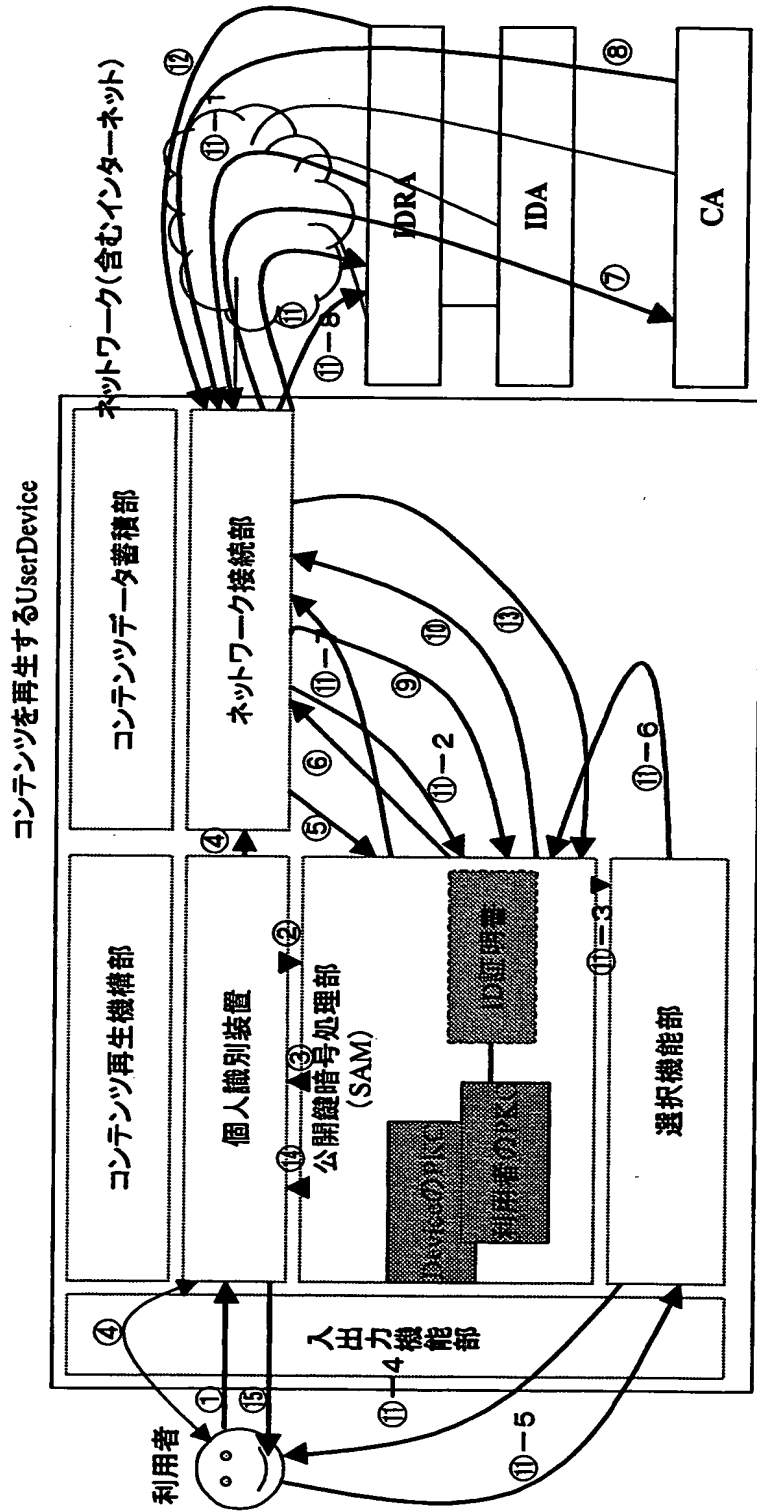
ユーザ登録、抹消、サービス契約におけるフローチャート(3)



【図 62】

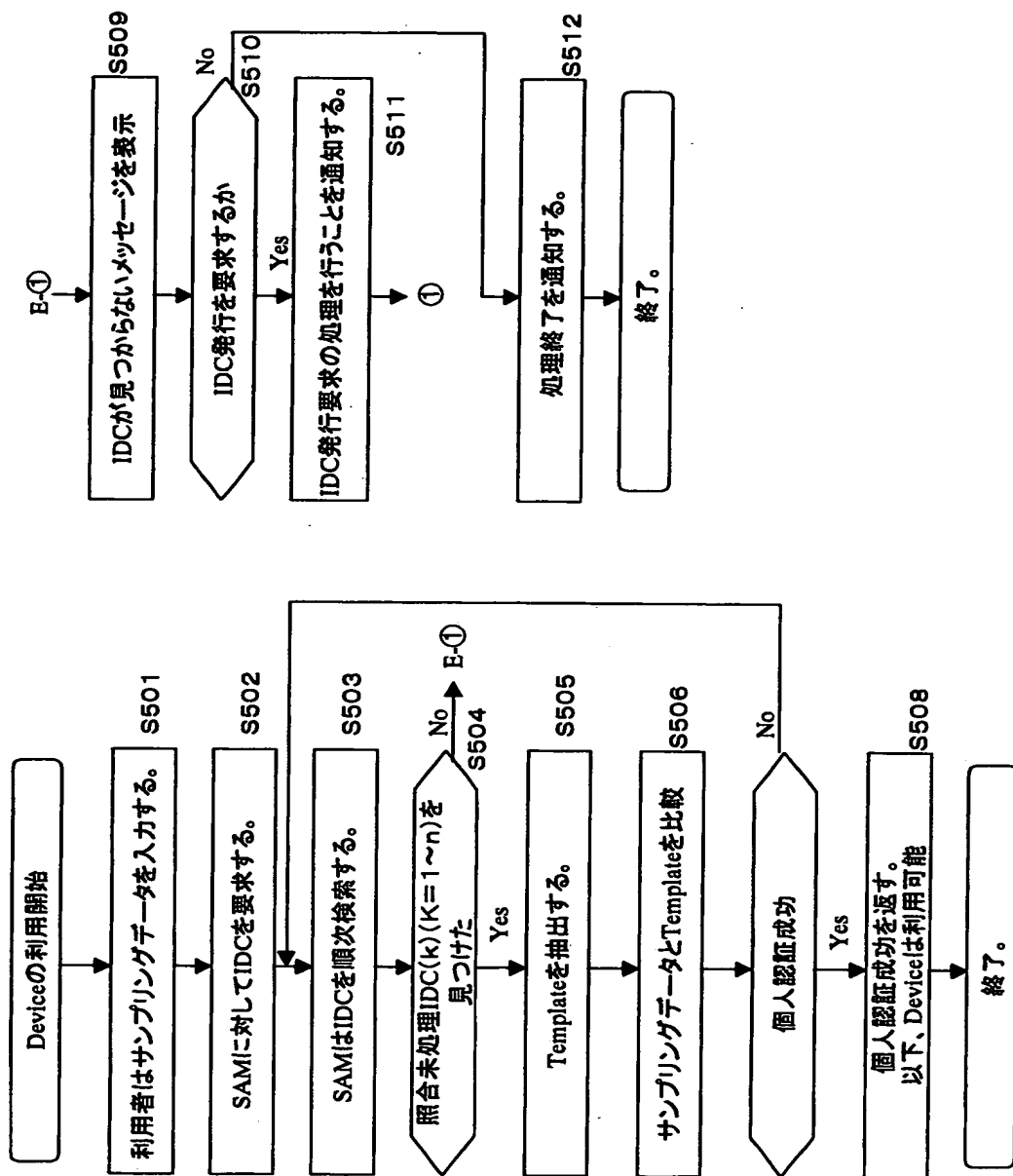
Device内に格納するIDCの要求

- 前提条件:
  - UserDeviceはIDCを未登録で、かつ、Templateを保有していない。
  - UserDeviceはPKCを未保持。鍵ペアを保有していないが、生成可能。
  - IDC発行に必要なOffline手続きは済ませてあることと、その際、申込者とTemplate提供者の一致を確認するための情報(PIN or Template情報そのもの or 秘密鍵による署名など)を設定し決定しているものとする。

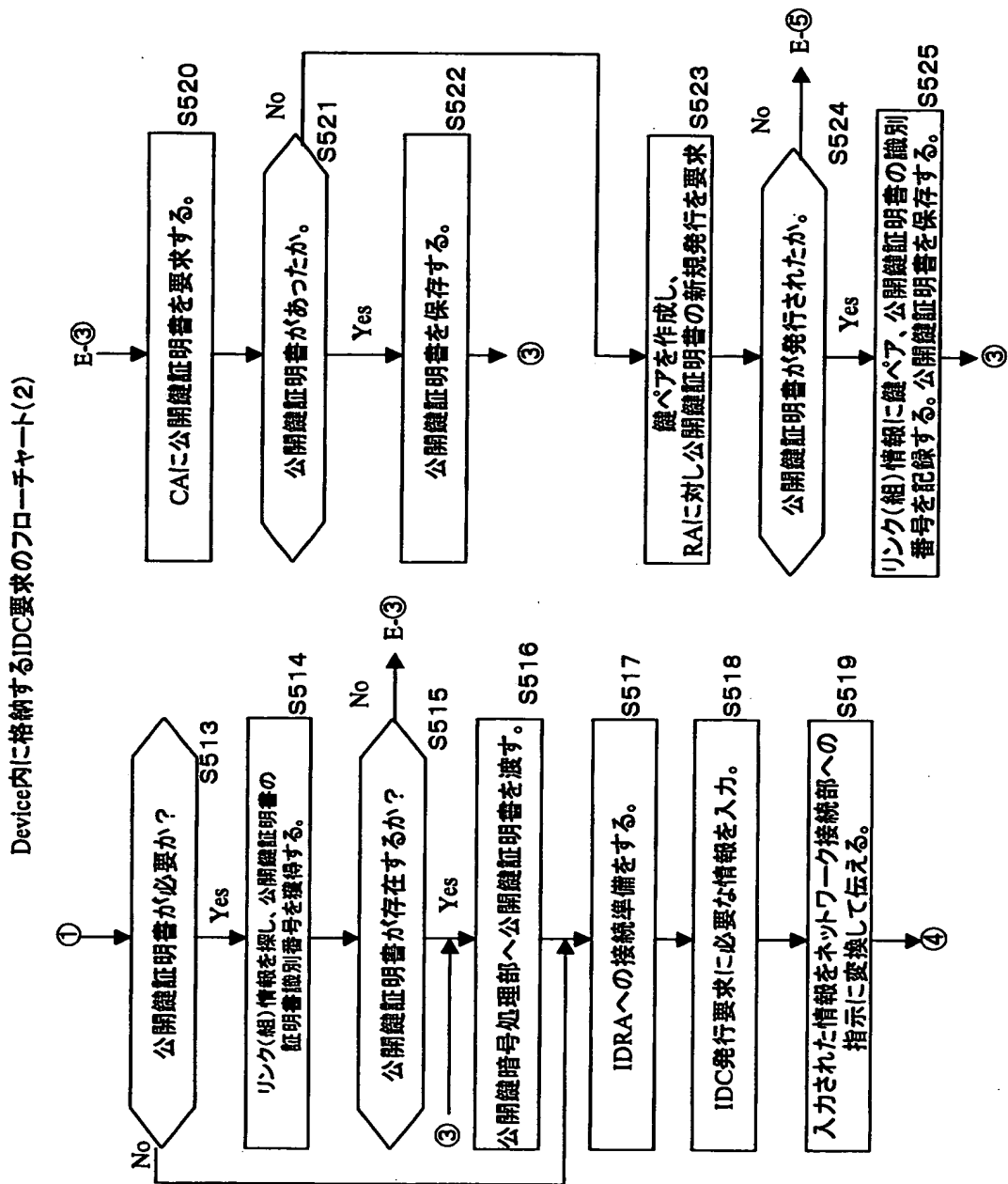


【図 63】

Device内に格納するIDC要求のフローチャート(1)

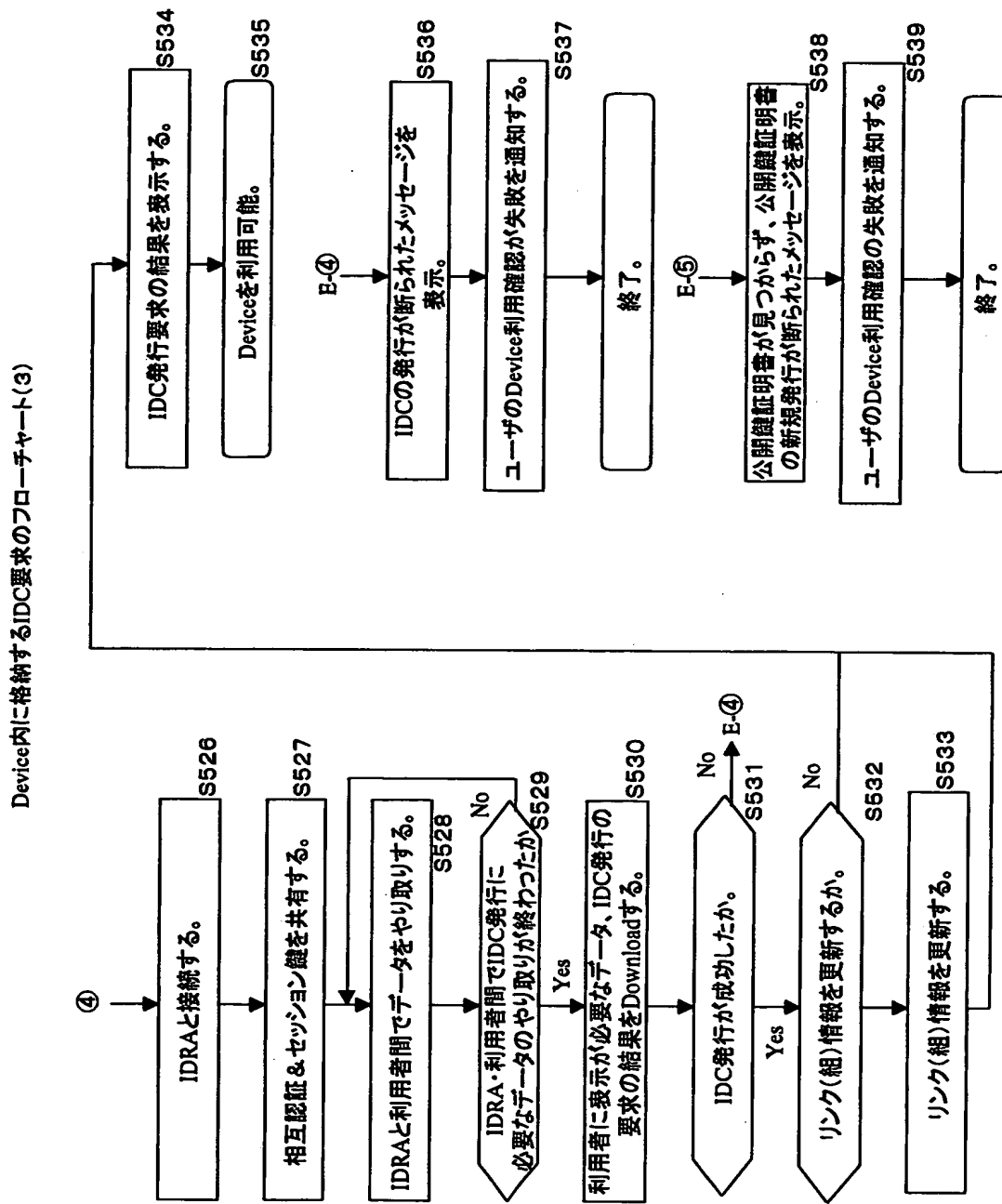


【図 6 4】

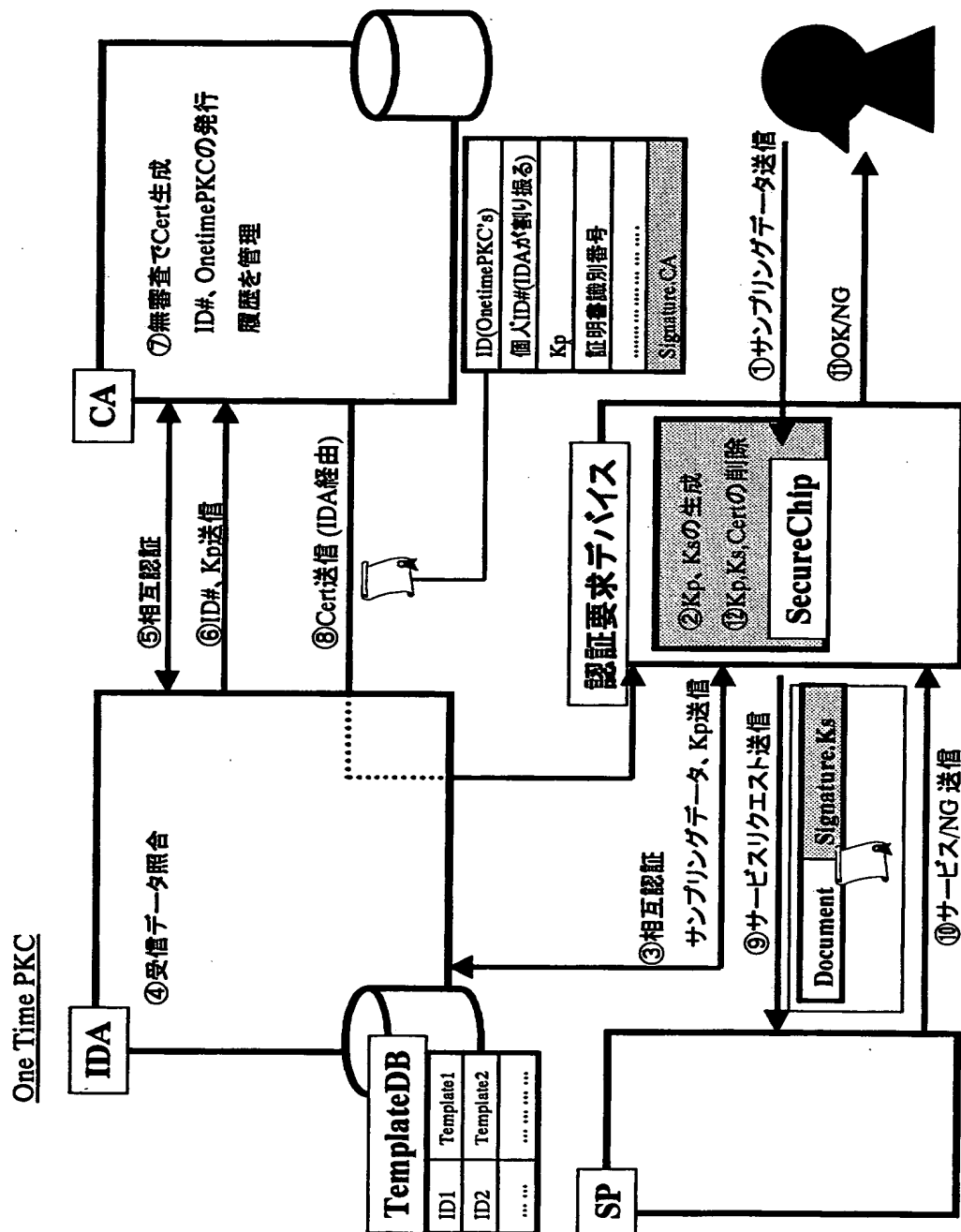




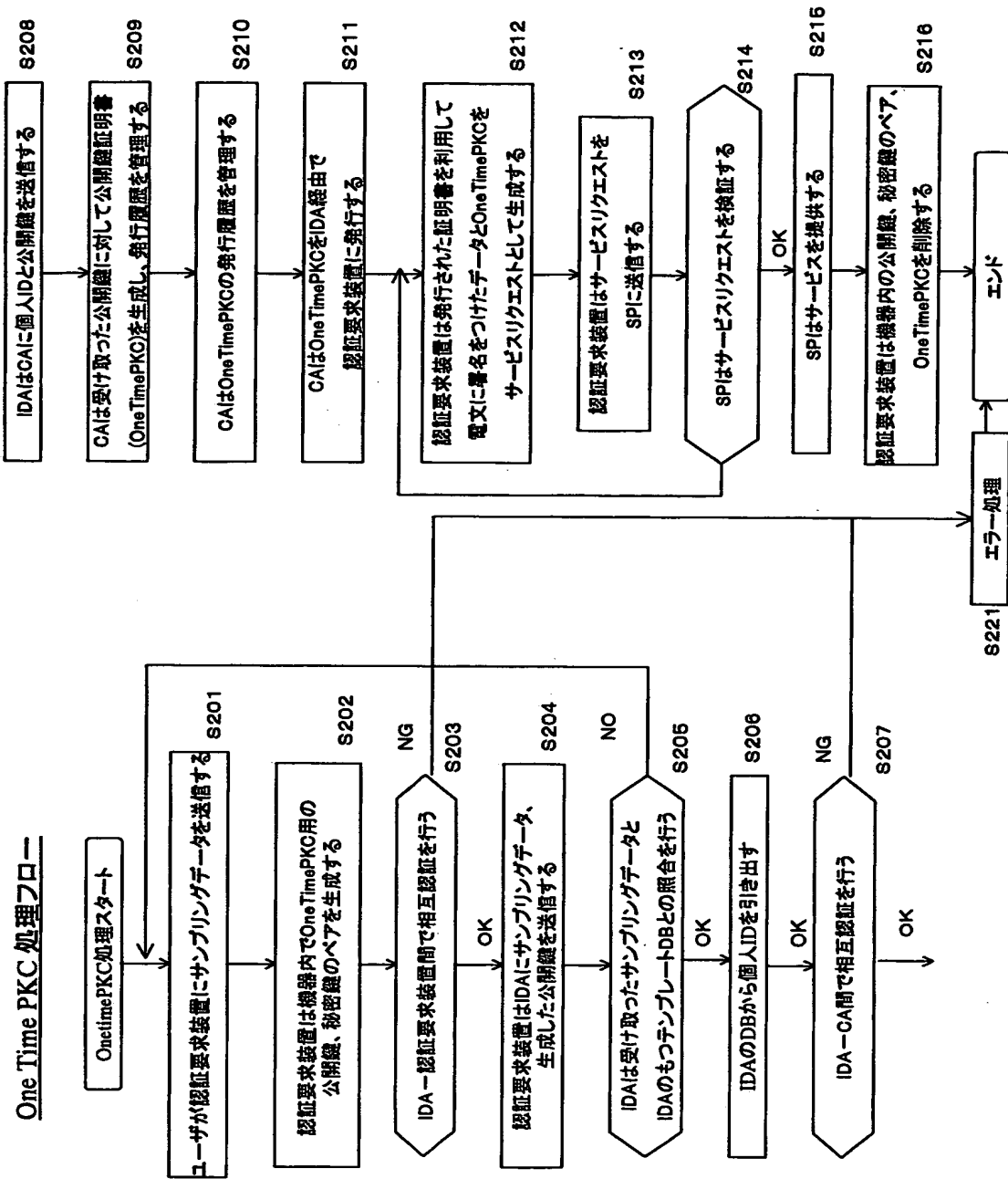
【図 6 5】



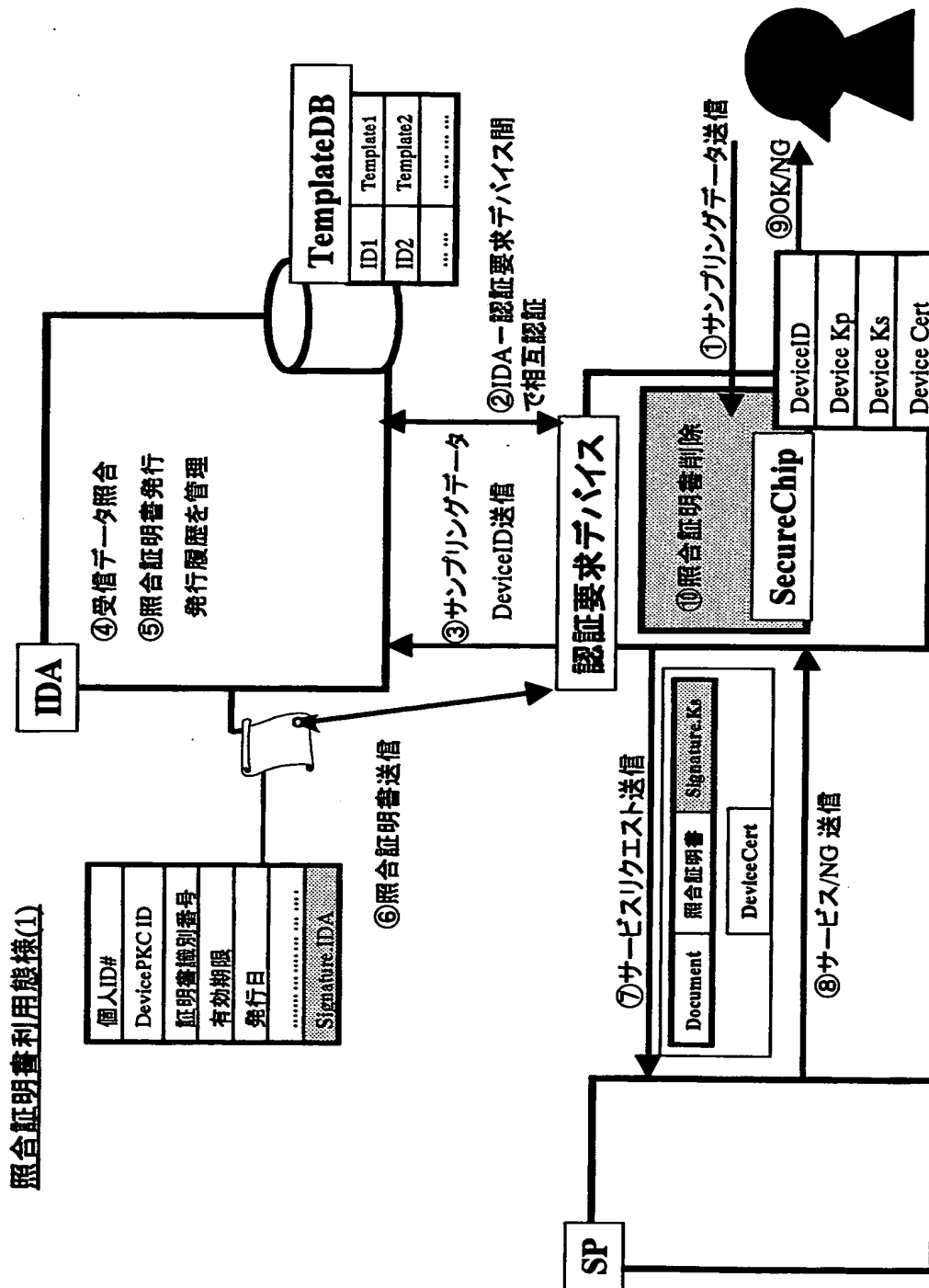
【図 66】



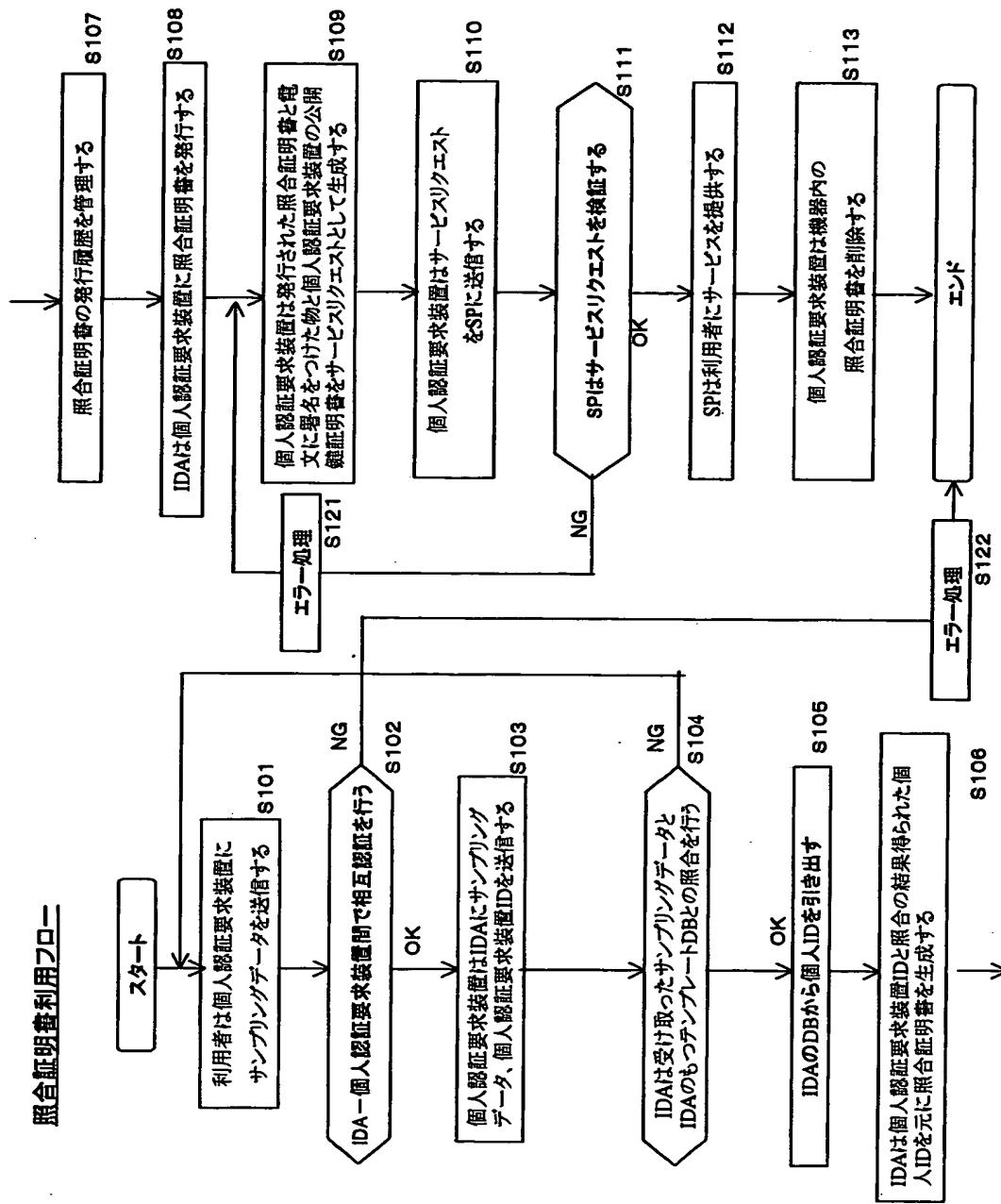
【図 6 7】



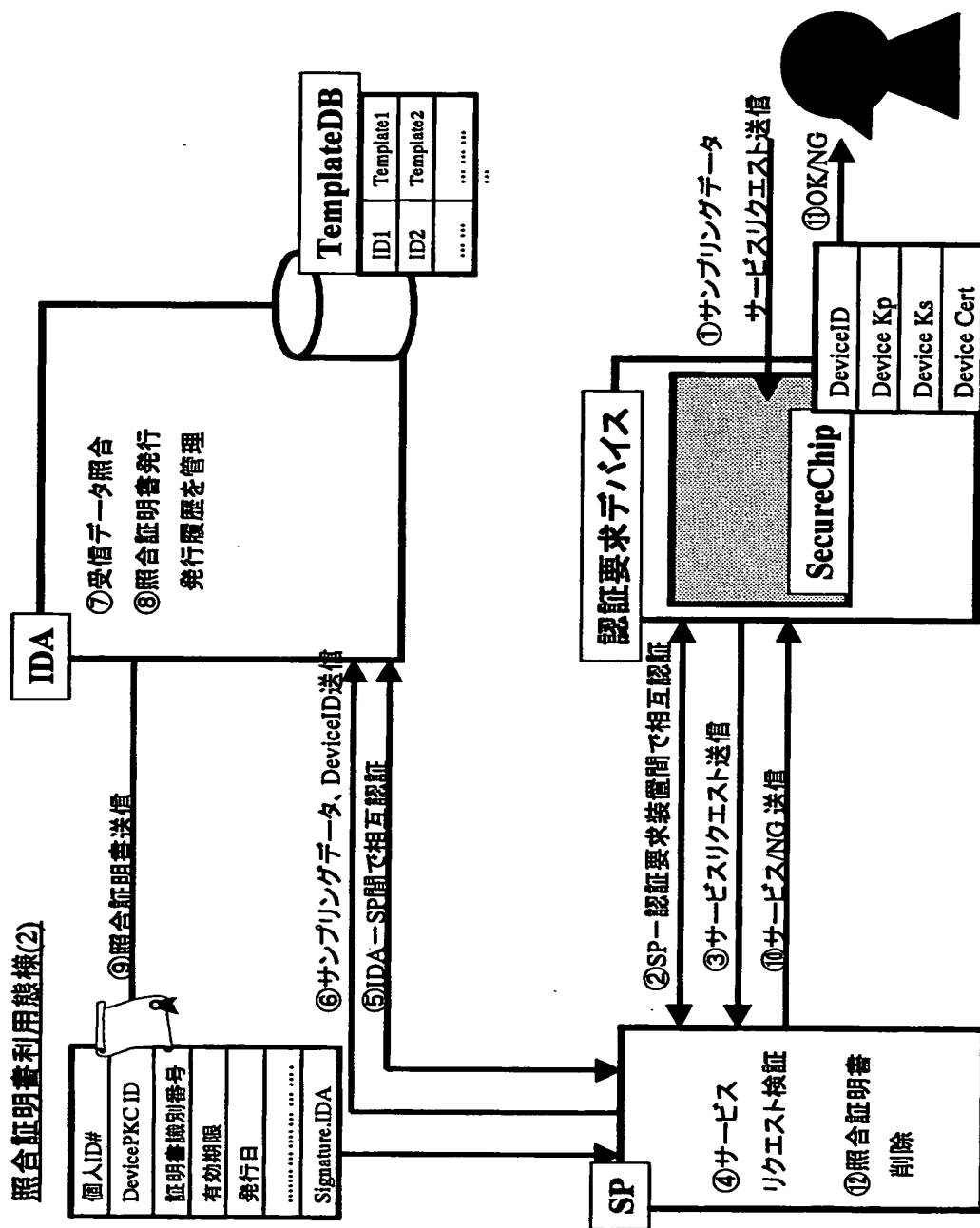
【图 6 8】



【図 69】



【図 7 0】



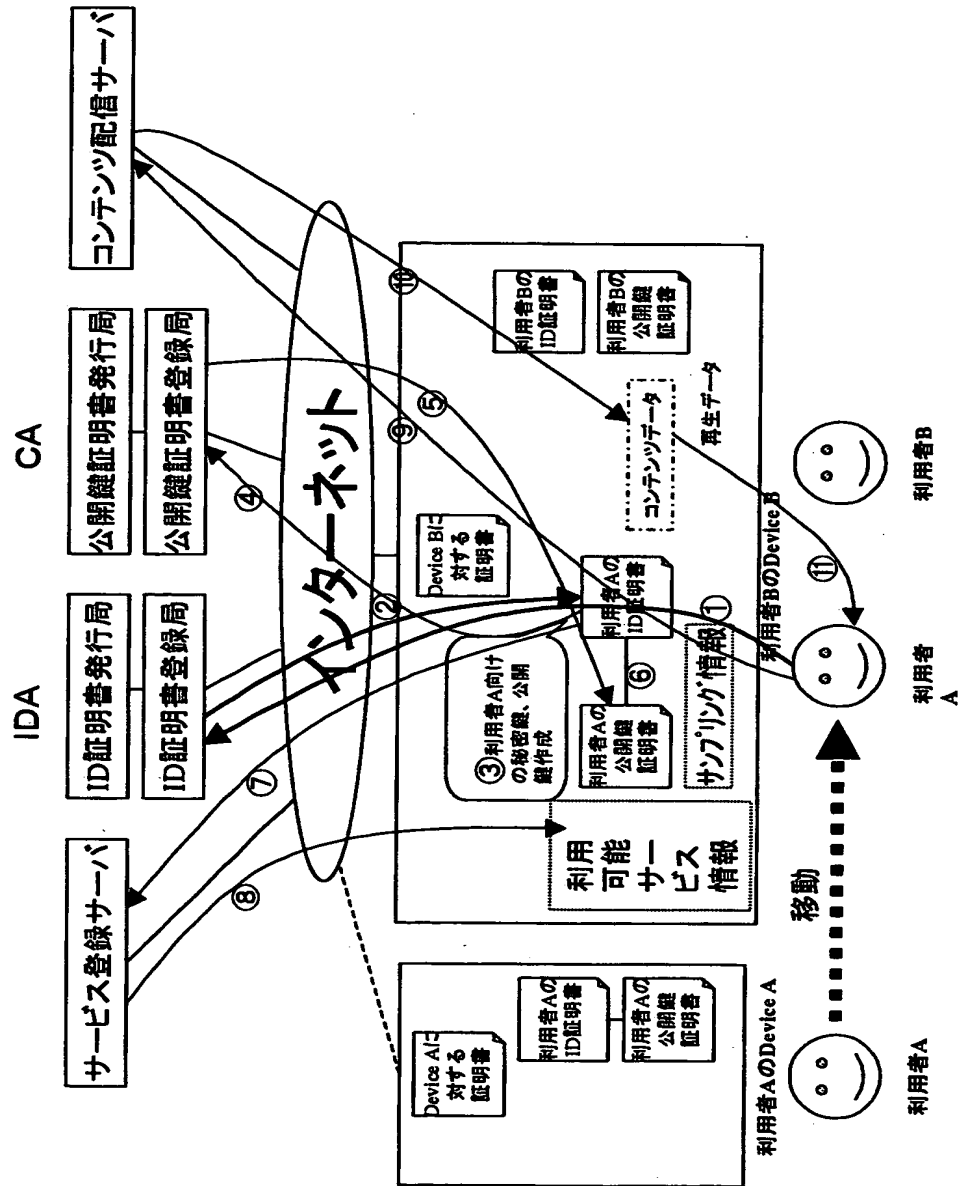
【図 7 1】

照合証明書フォーマット

| 項目   | 説明   |
|--|--|
| Version  | バージョン  |
| SerialNumber   | 認証番号   |
| signaturealgorithmIdentifier<br>algorithm<br>parameters        | 署名方式<br>アルゴリズム<br>パラメータ  |
| Issuer   | 個人識別認証局名(Distinguished Name形式)                                   |
| Validity<br>notBefore<br>notAfter                              | 有効期限<br>・ 開始日時<br>・ 終了日時   |
| subject  | 被認証者名(DN形式)  |
| subjectIDAInfo<br>subjectIDAserialNumber<br>subjectIDAUniqueID | 被認証者の個人識別証明書情報<br>・ 被認証者の個人識別証明書の認証番号<br>・ 被認証者の個人識別証明書の被認証者固有ID |
| subjectPKCinfo<br>subjectPKCserialNumber<br>subjectPKCUniqueID | 被認証者の公開鍵証明書情報<br>・ 被認証者の公開鍵証明書の認証番号<br>・ 被認証者の公開鍵証明書の被認証者固有ID    |
| 必 須 項 目  | 必 IDASignature   |
|  | IDAの署名   |

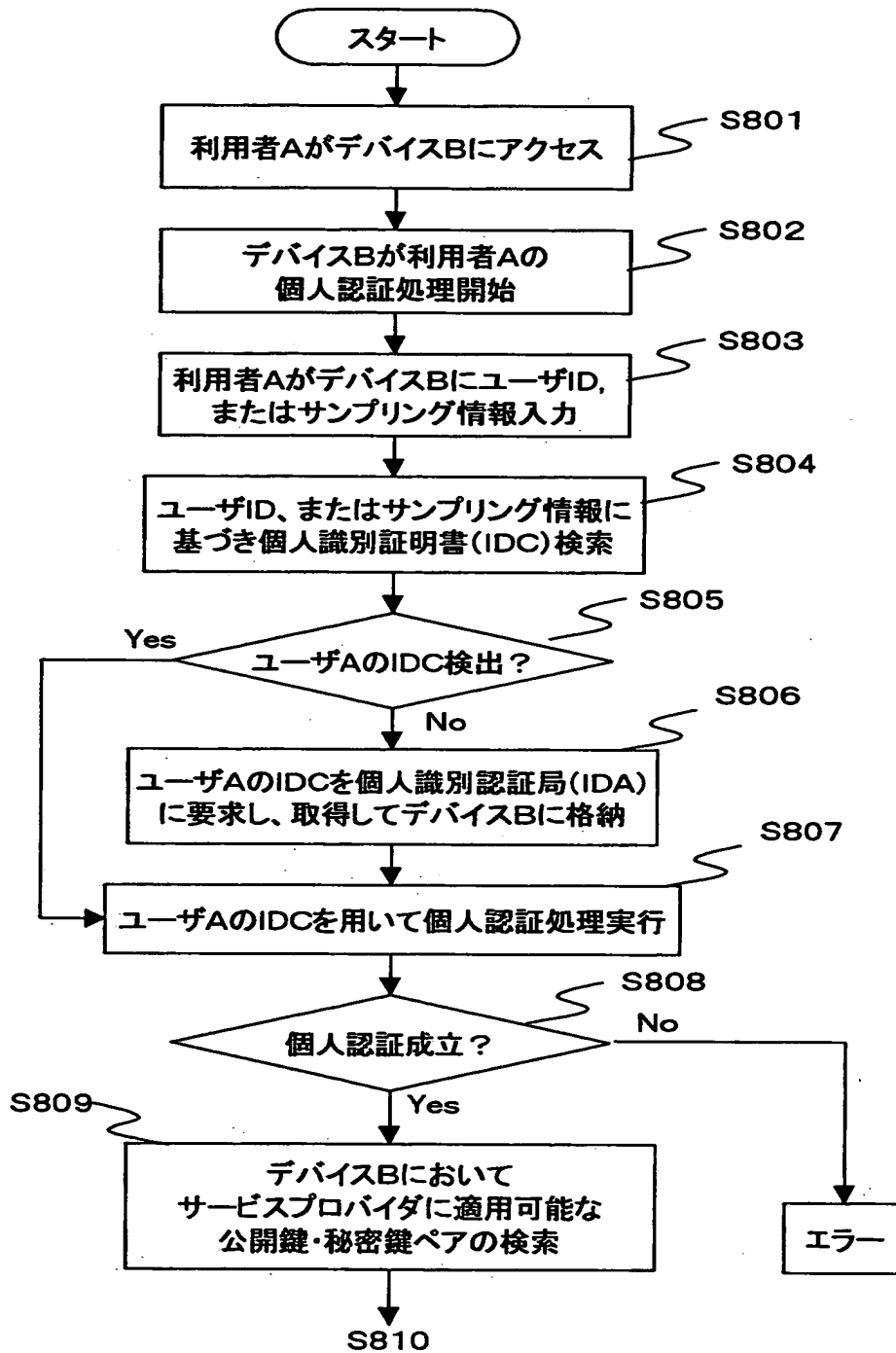
【図 7 2】

状況：利用者のIDCが無いDeviceで使用する。  
方法1) IDCとリンクしたPKCを追加してサービス利用

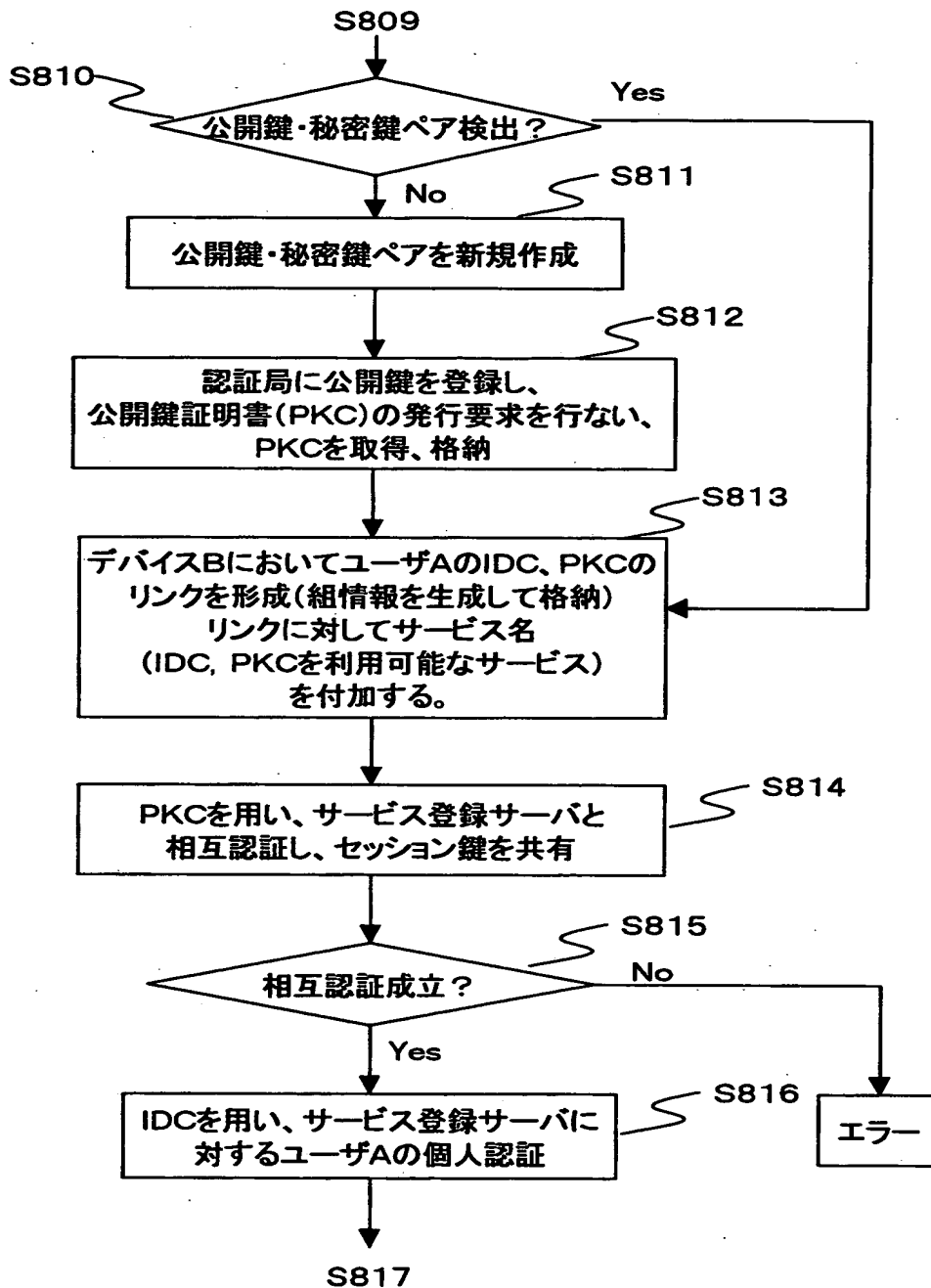




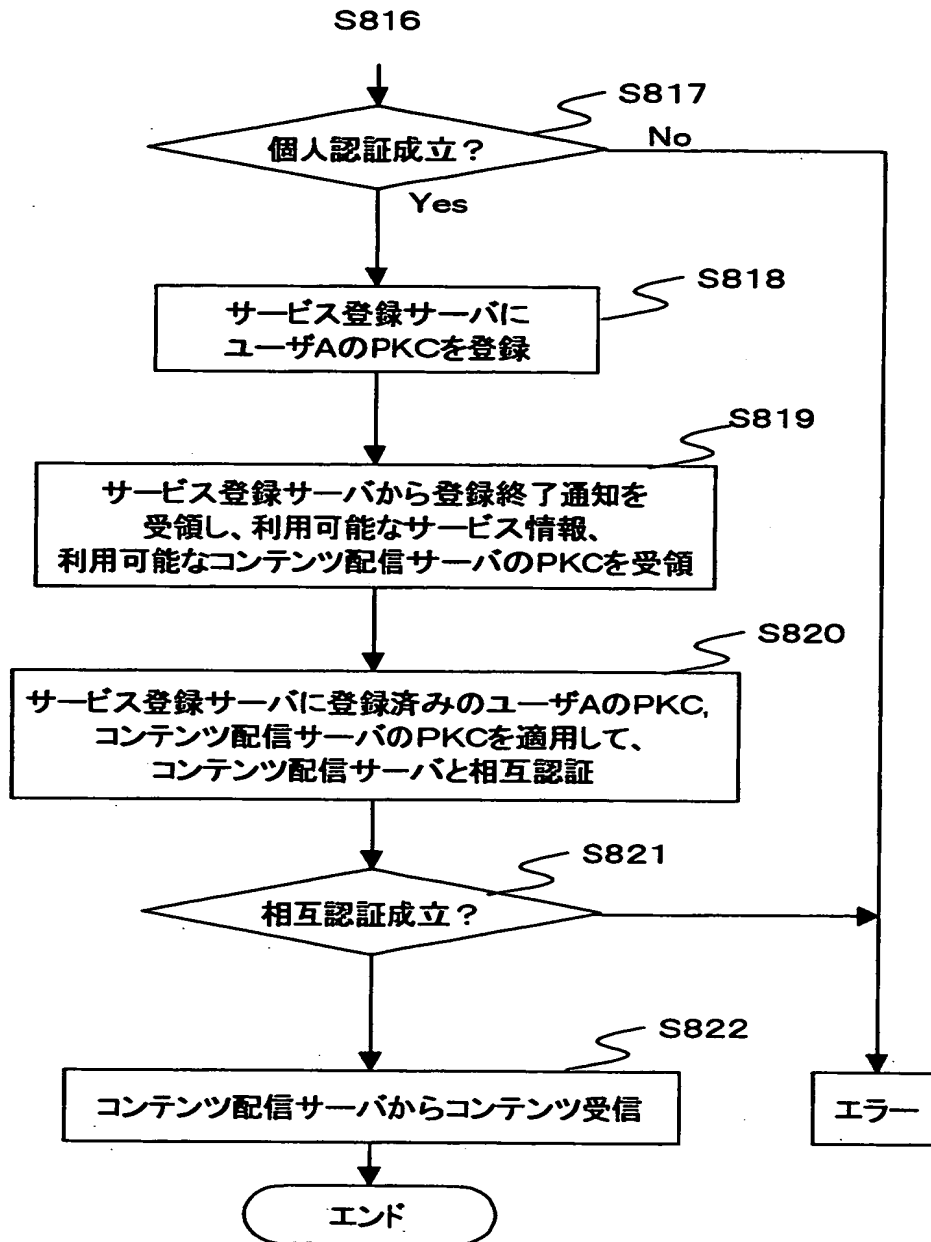
【図 73】



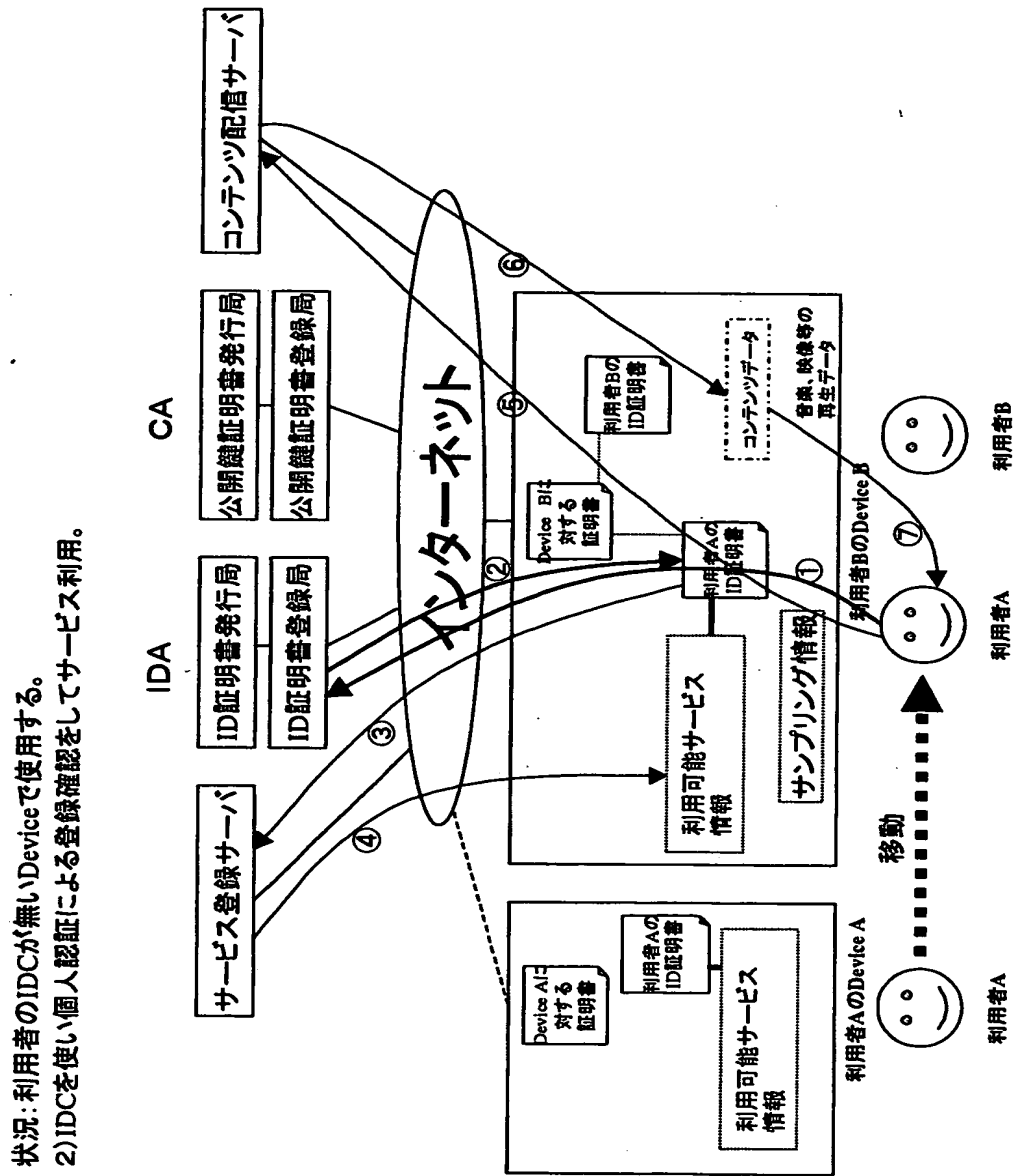
【図 74】



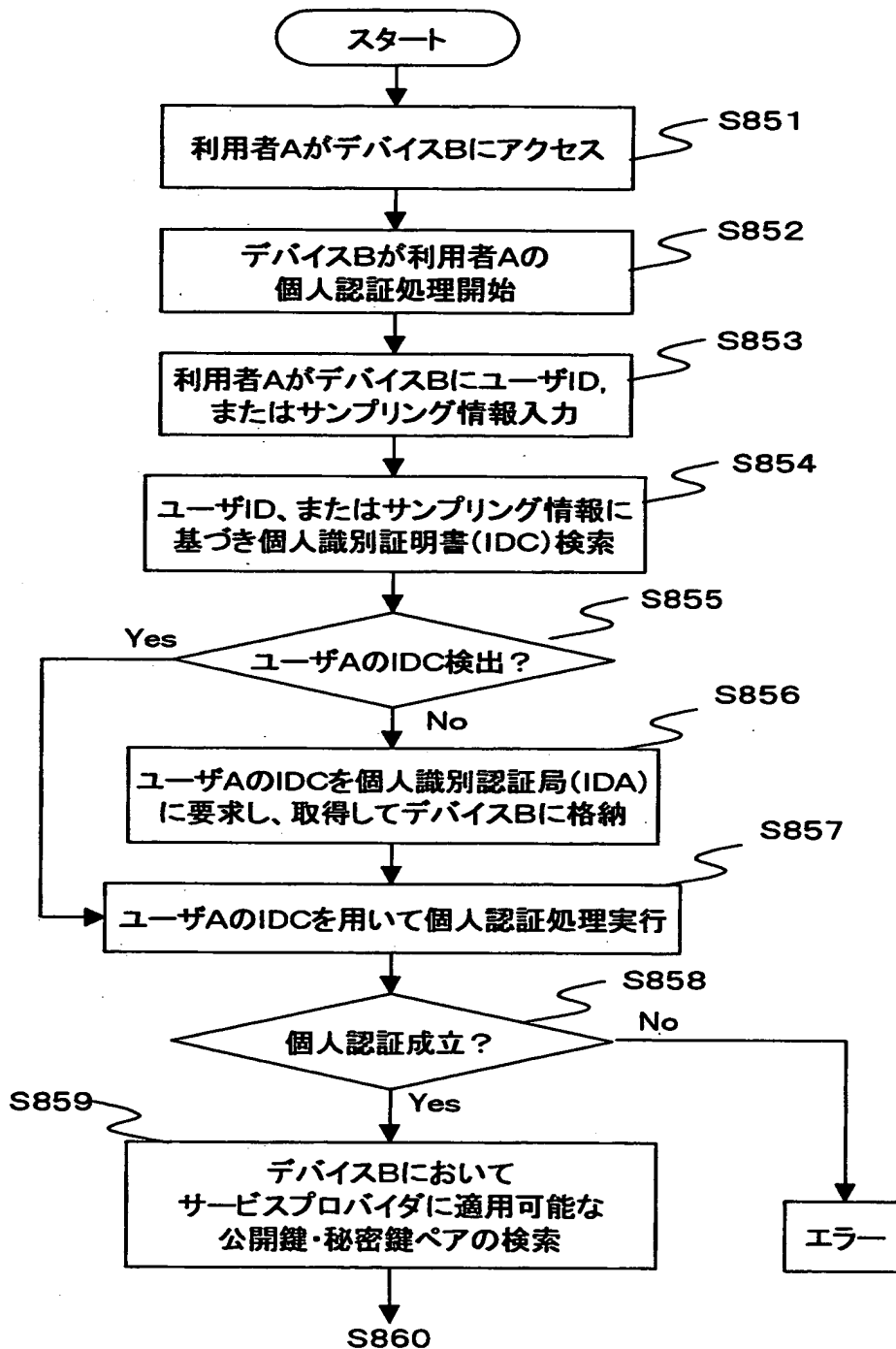
【図 75】



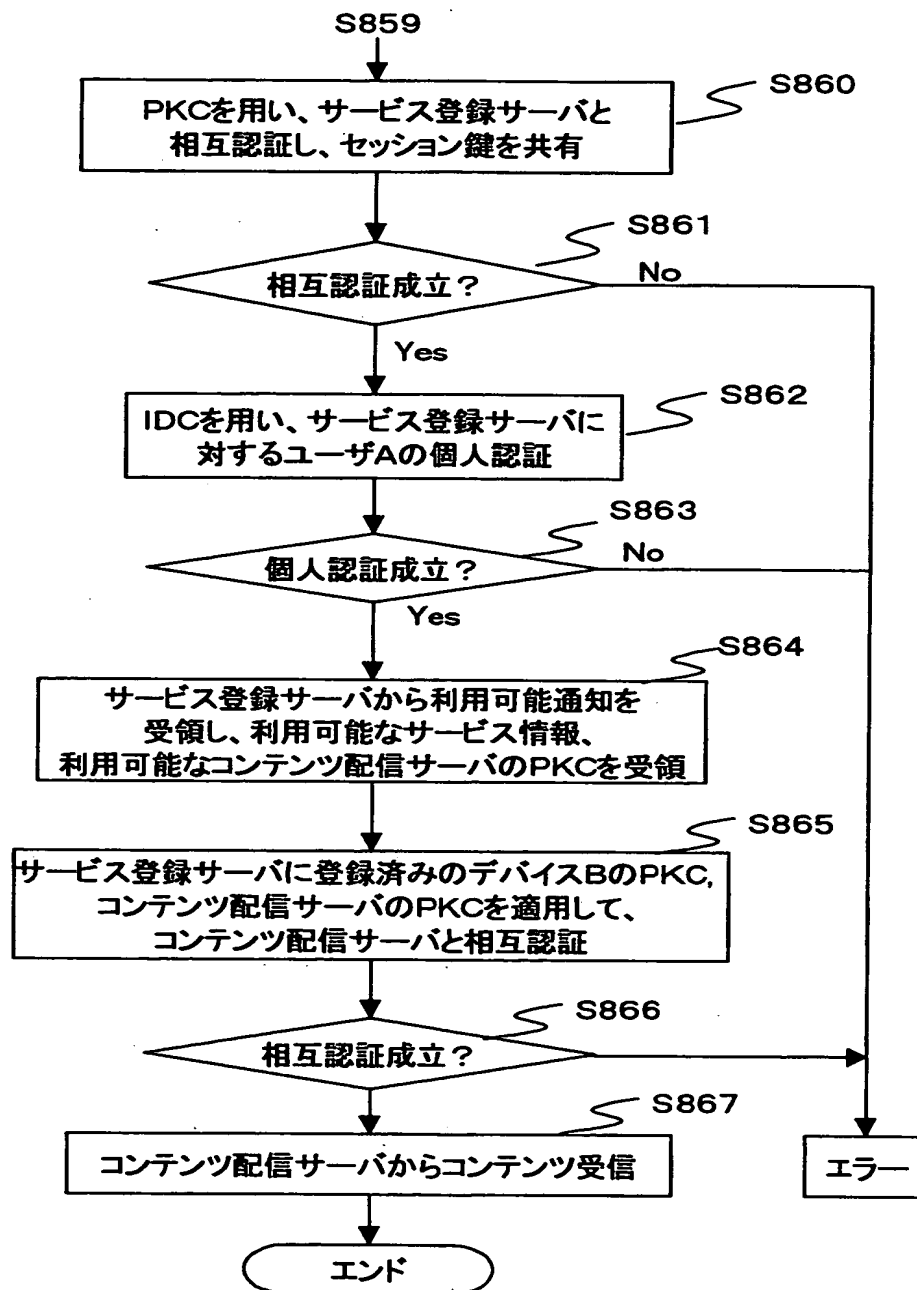
【図 76】



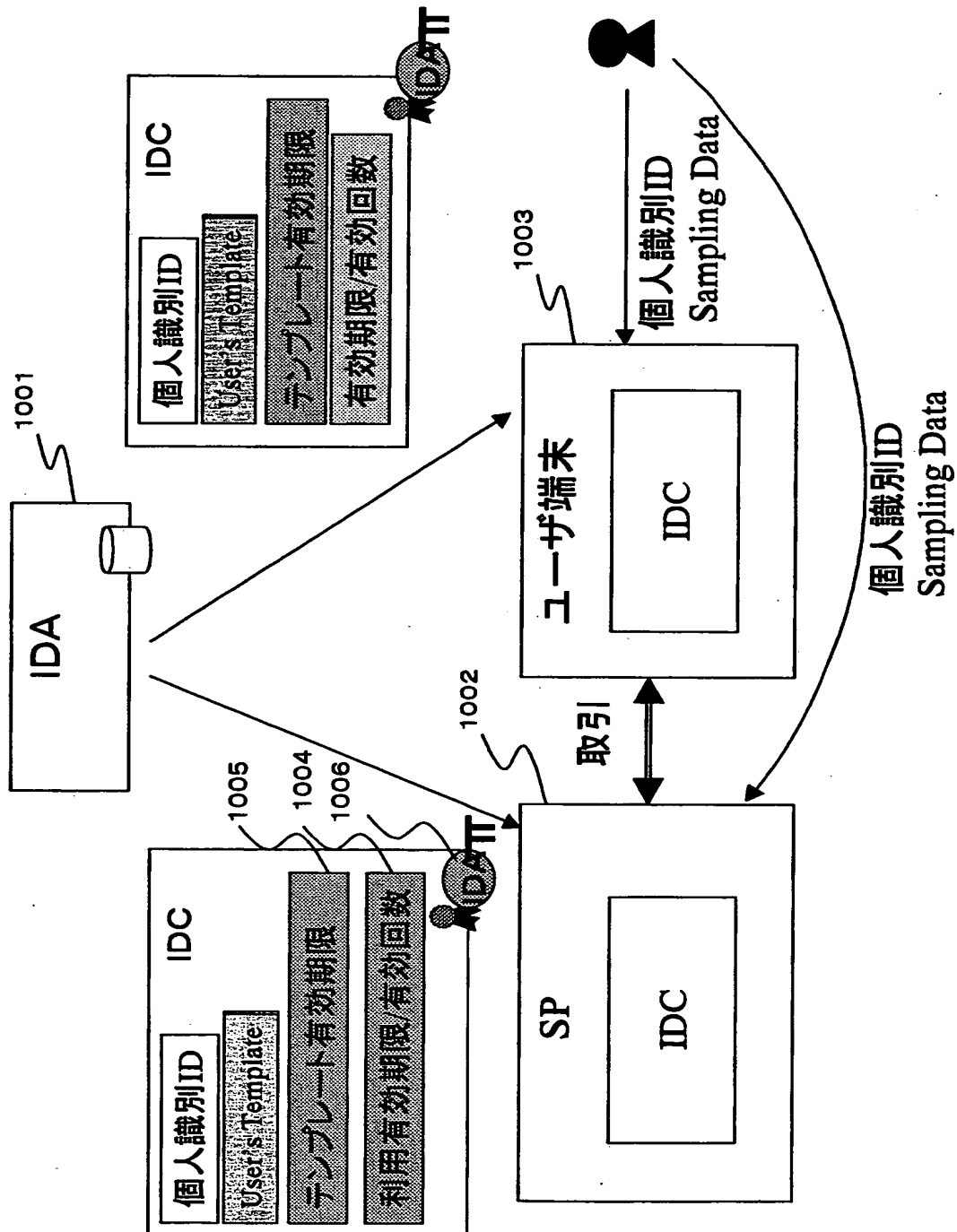
【図 77】



【図 78】

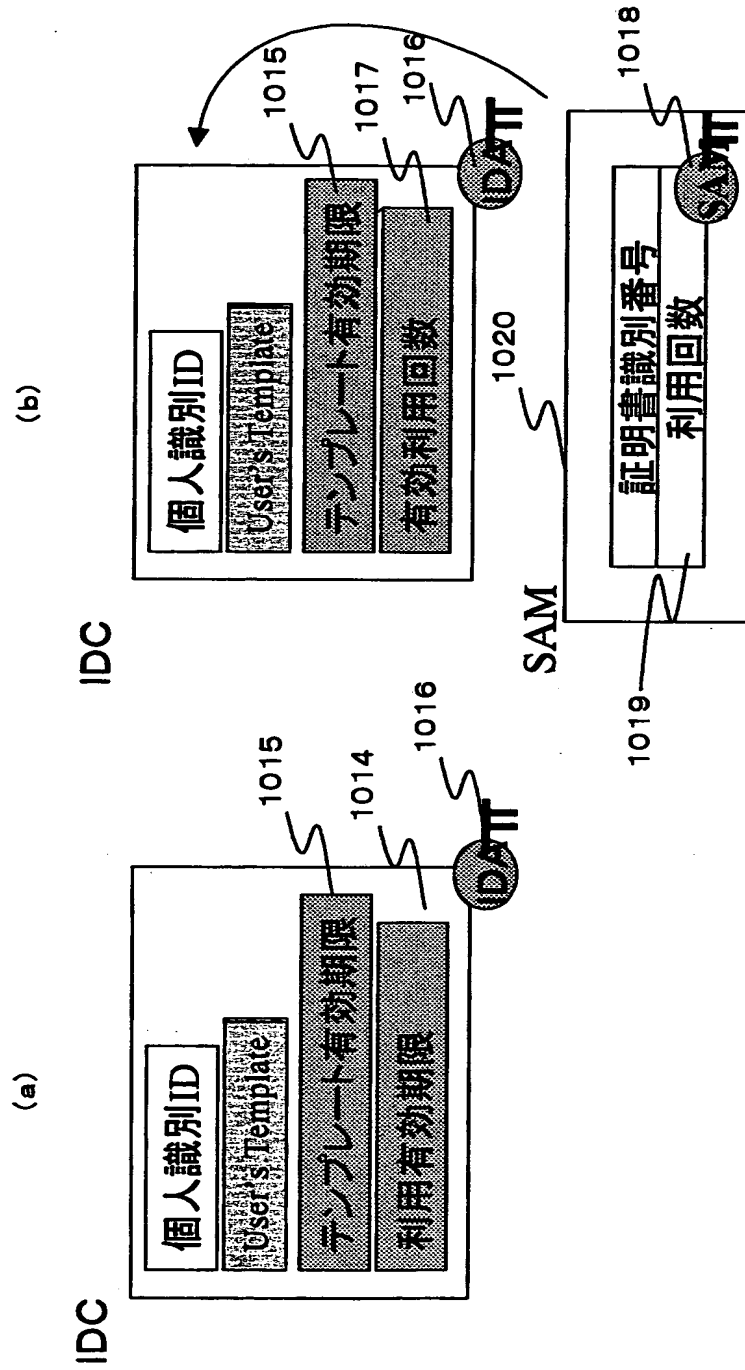


【図79】



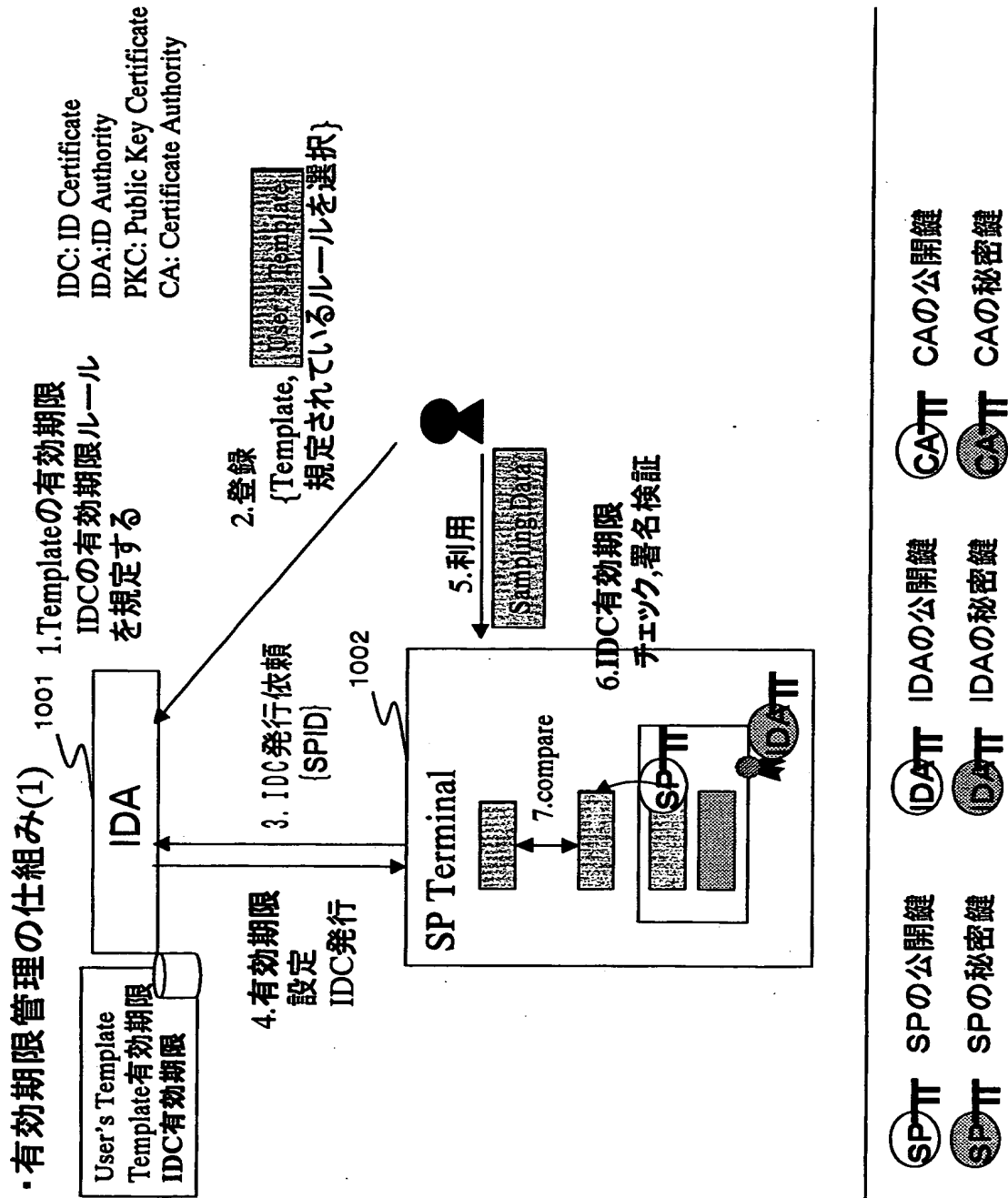
【図 80】

- ・有効情報
- ・テンプレート有効期限
- ・IDC利用有効情報（有効期限／有効利用回数）＜テンプレート残りの有効期限

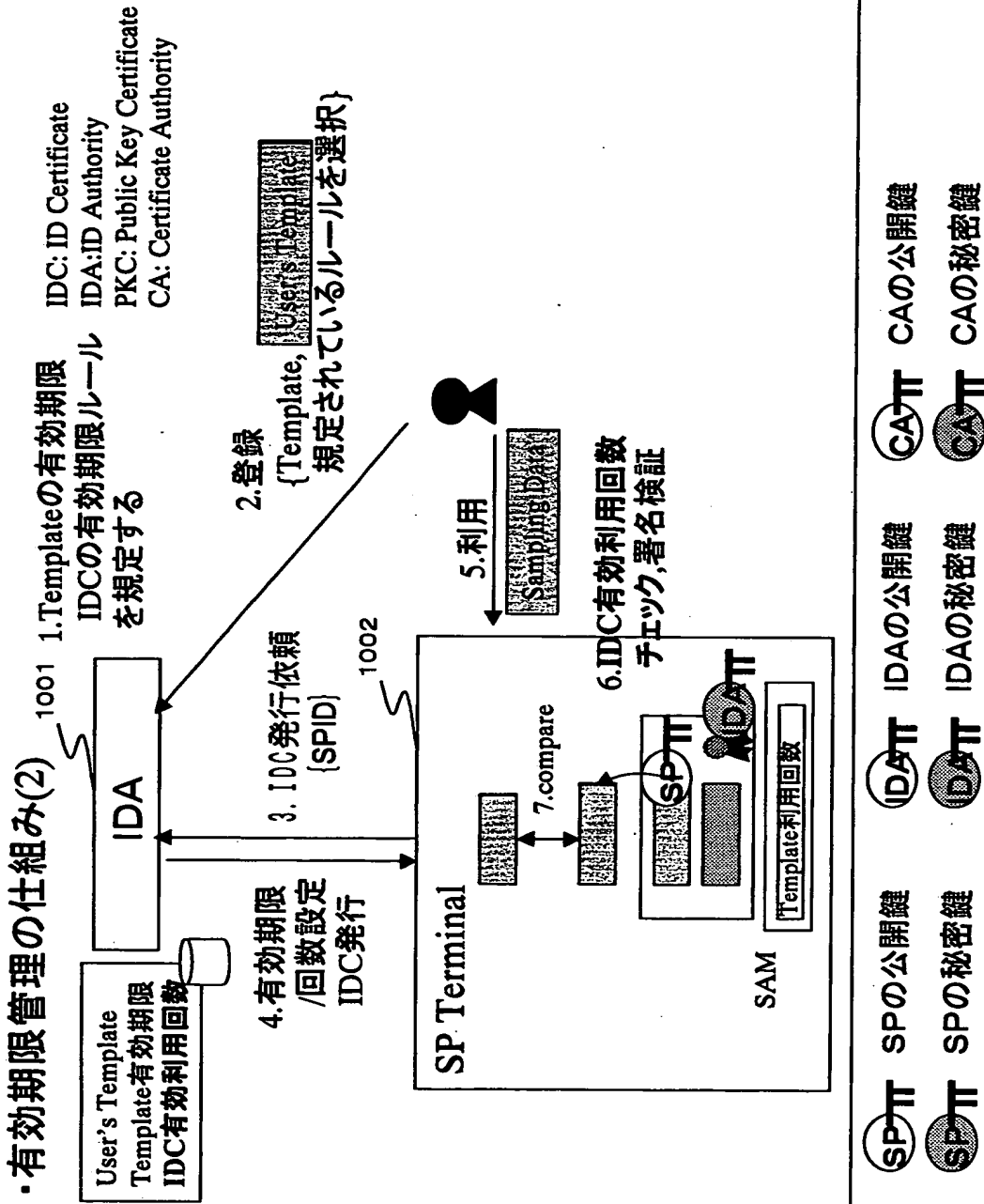




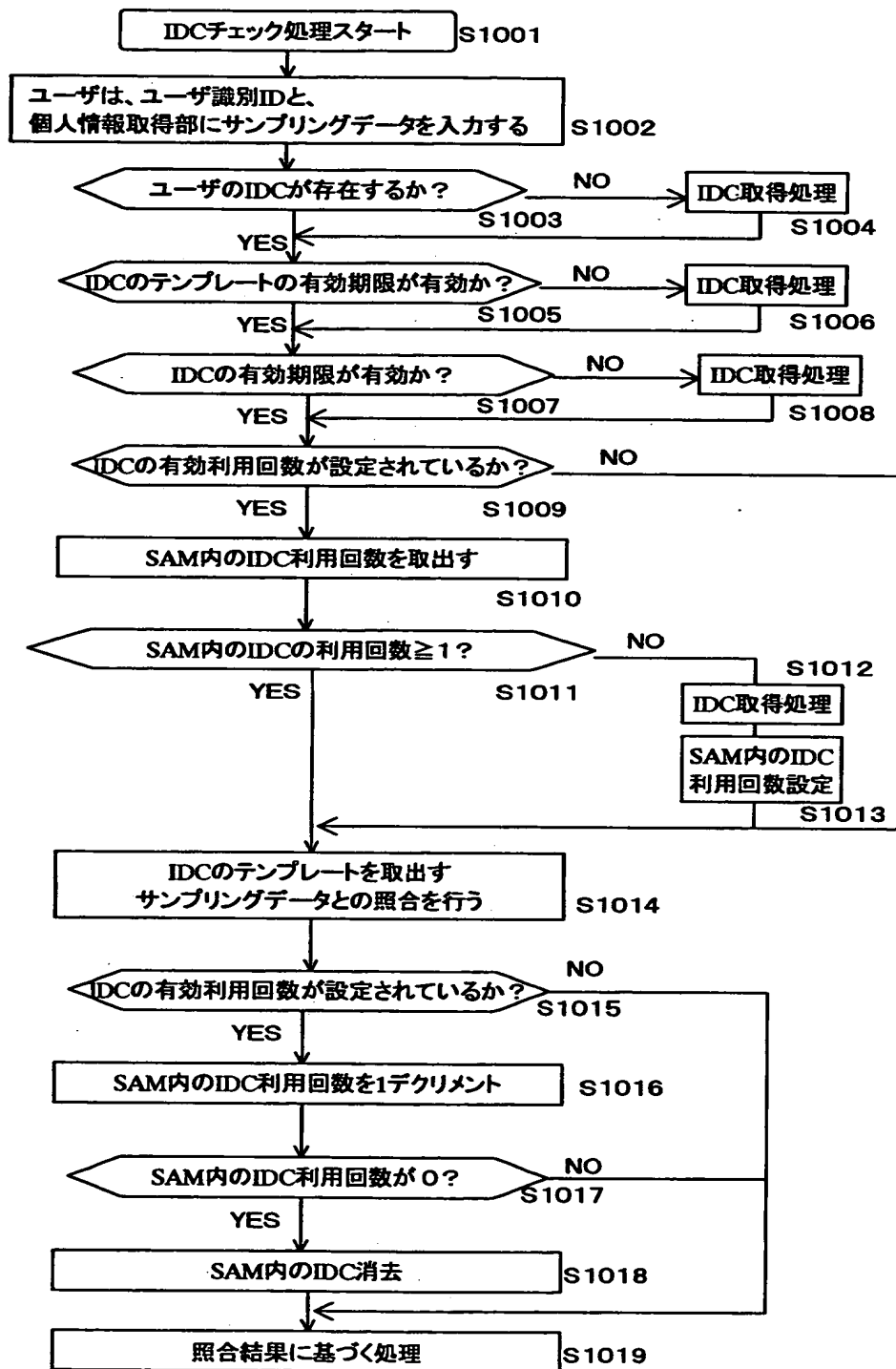
【図 8 1】



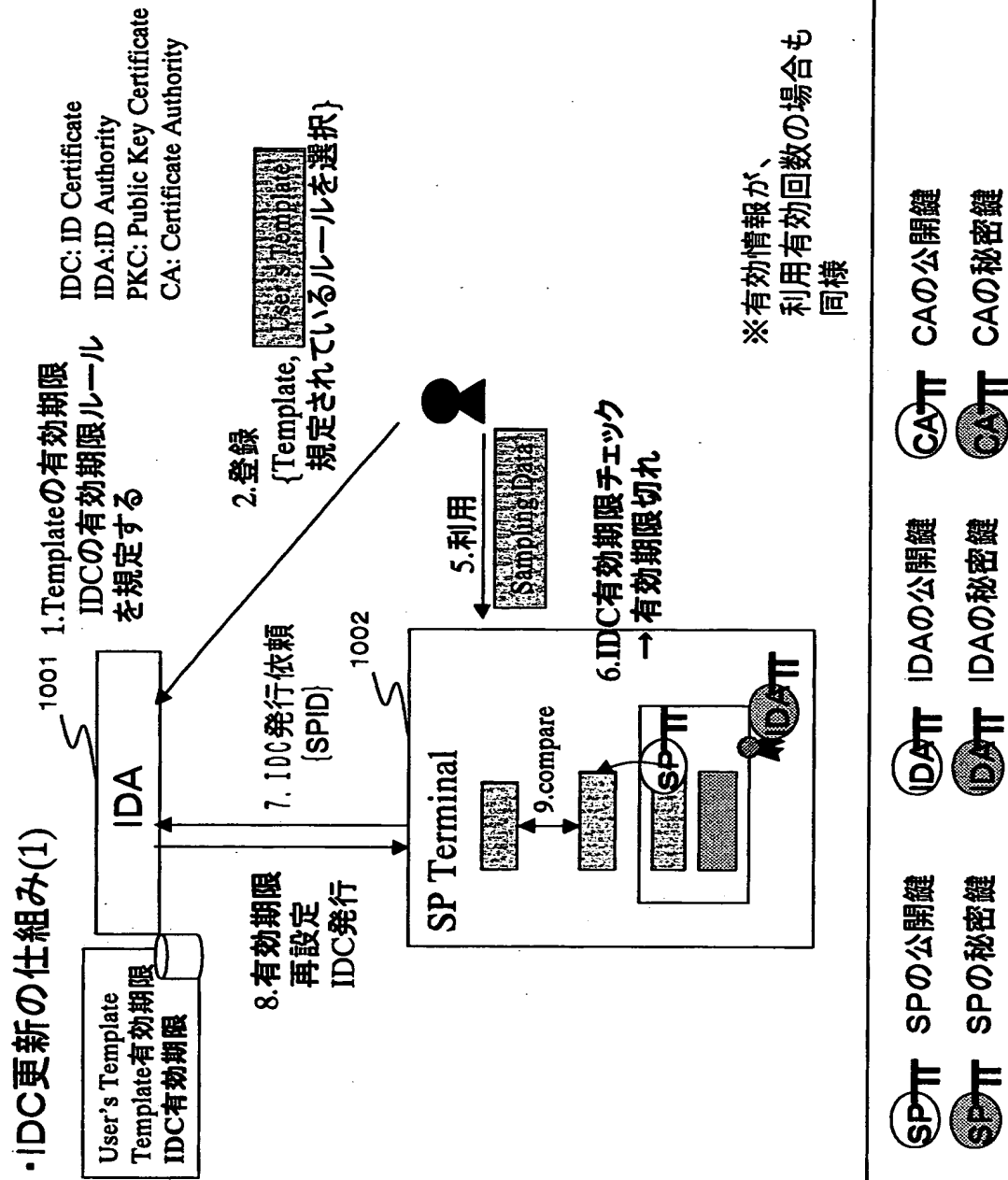
【図 82】



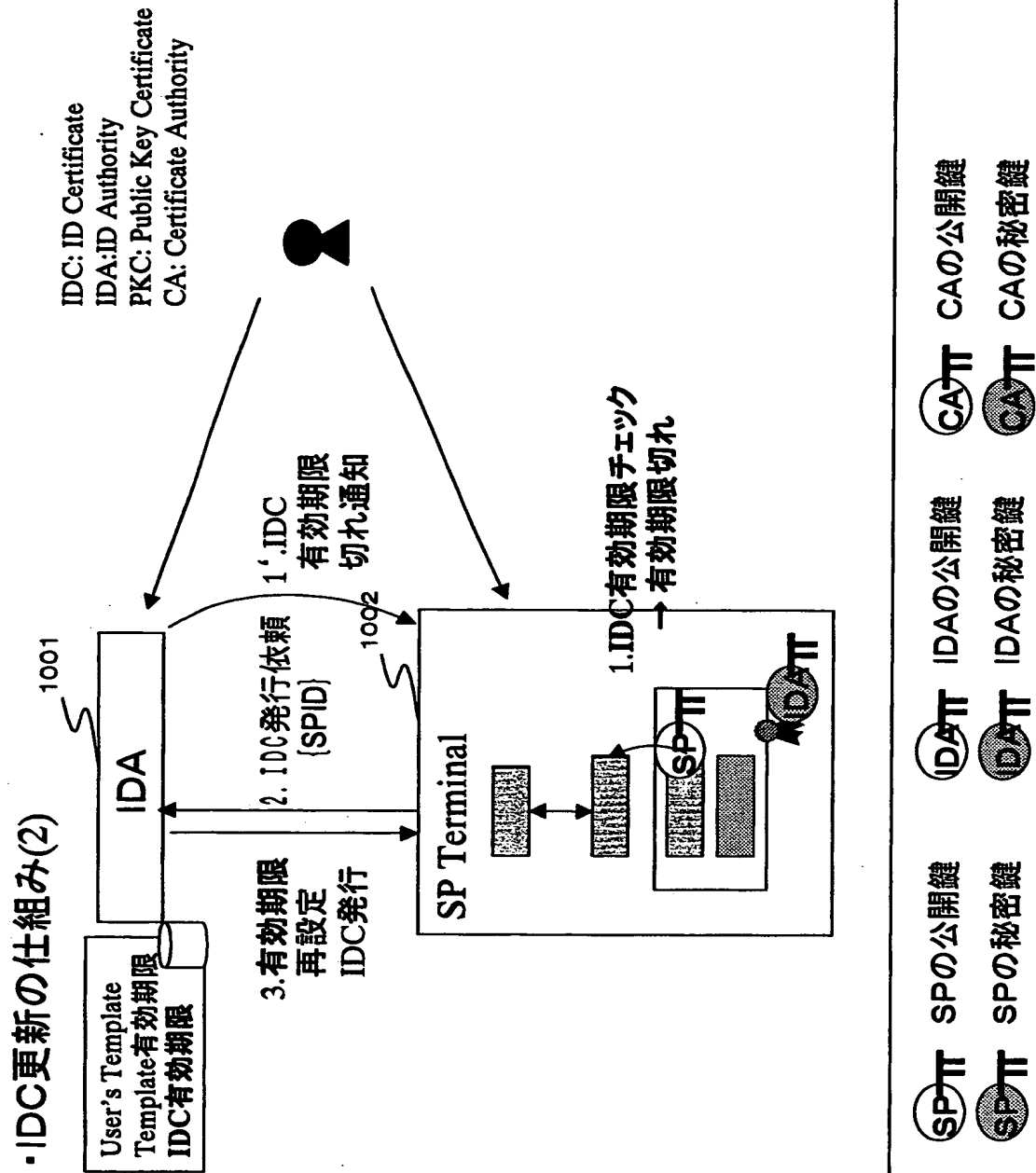
【図 83】



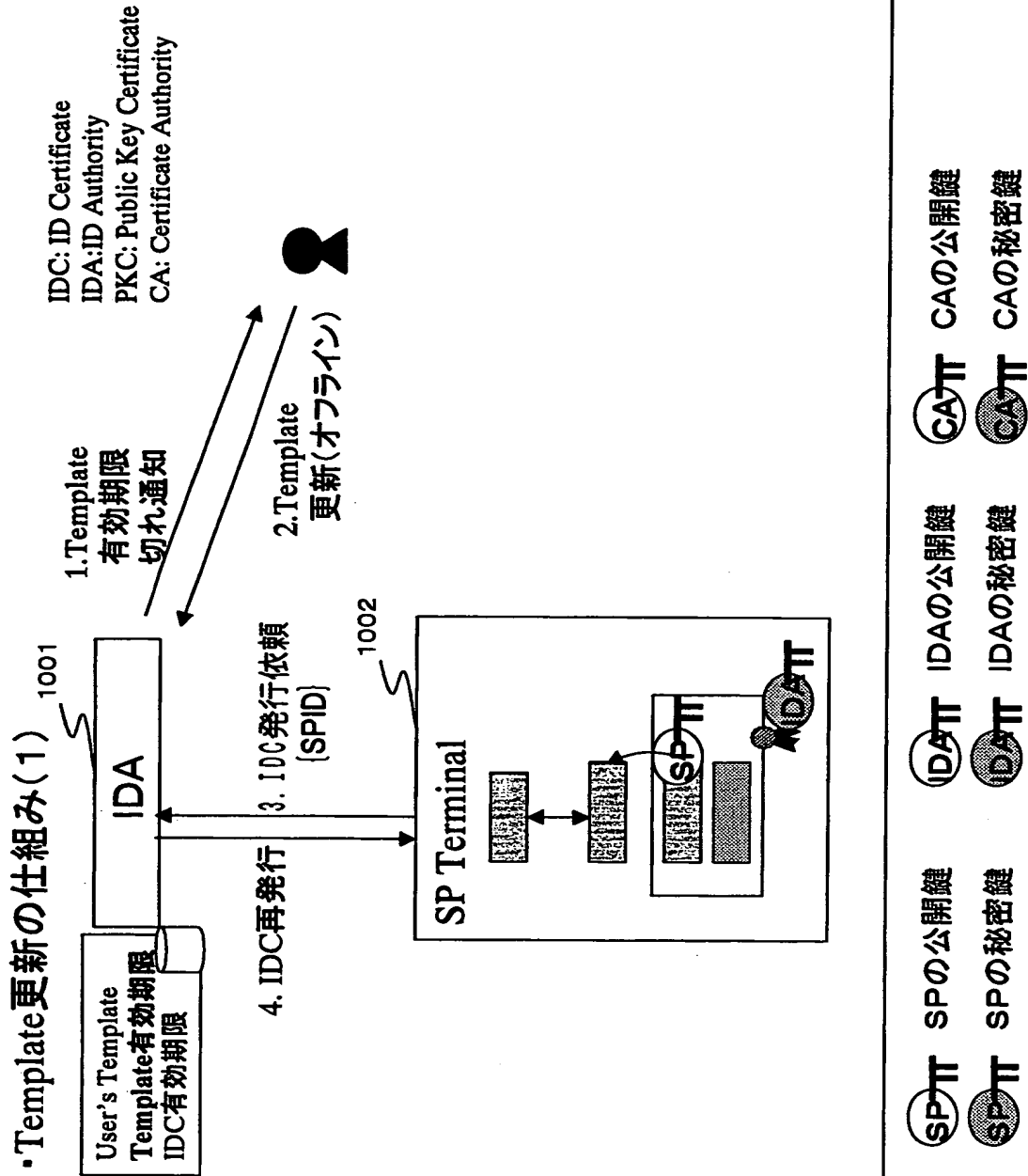
【図 84】



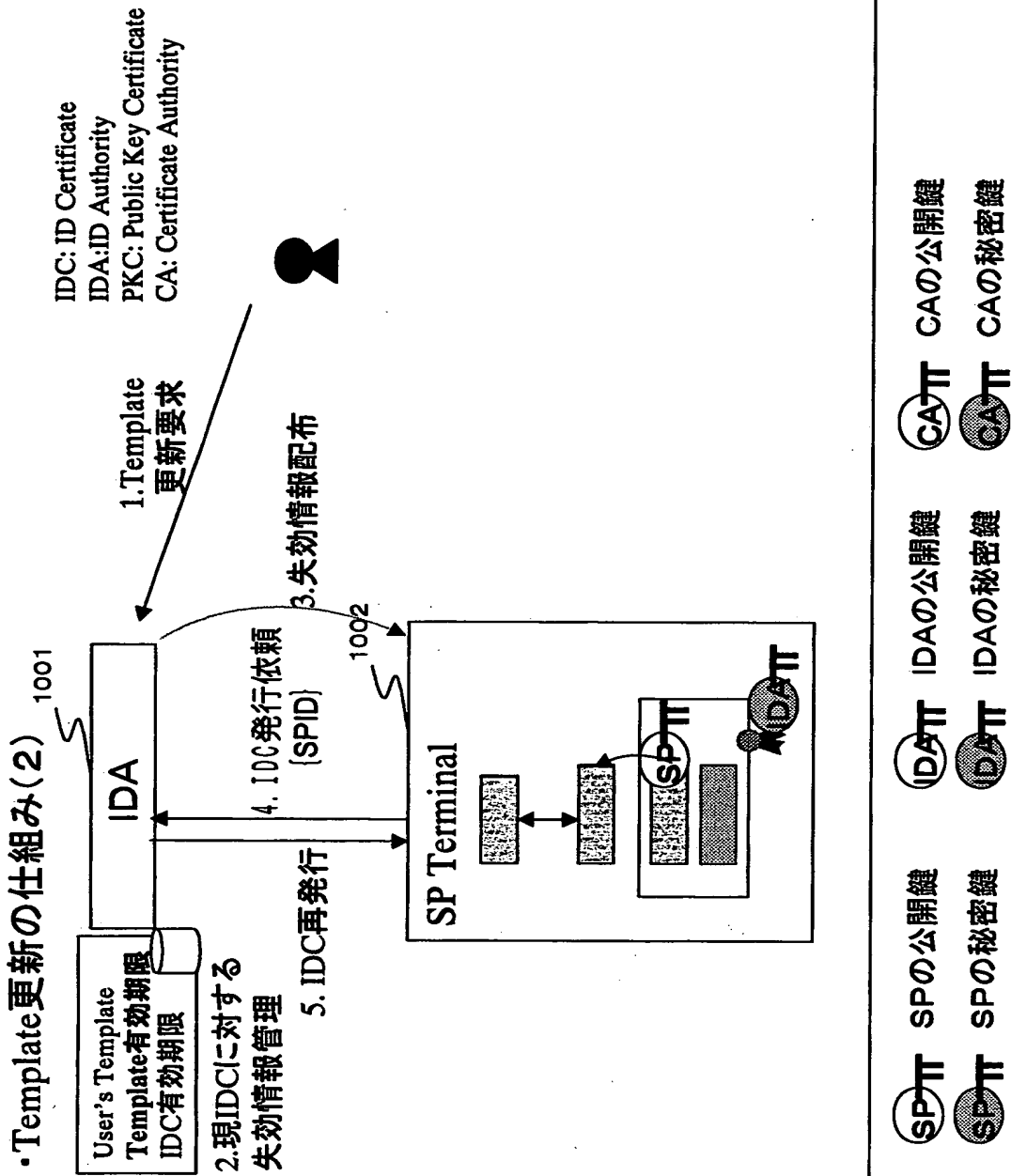
【図 85】



【図 86】



【図 87】



【書類名】 要約書

【要約】

【課題】 迅速に公開鍵証明書を発行し、利用することの可能な公開鍵証明書利用システムを提供する。

【解決手段】 公開鍵証明書の発行要求者の個人識別データとしてのテンプレートを個人識別証明書から取得し、テンプレートとサンプリング情報との照合処理により個人認証を実行し、個人認証の成立を条件として、要求者の公開鍵証明書を発行する。公開鍵証明書を発行する認証局は、個人識別認証局の個人認証の成立を条件として公開鍵証明書を発行することが可能となるので、認証局における個人確認処理負担が軽減される。ユーザに対して発行される公開鍵証明書は、公開鍵証明書の利用処理完了に伴い削除処理が実行され、特有の処理においてのみ利用可能な構成が実現される。

【選択図】 図 6 6



特2000-264521

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都品川区北品川6丁目7番35号  
氏 名 ソニー株式会社